Ruckus Wireless™ ZoneFlex™ Outdoor Access Point

Release 9.4 User Guide

For the following ZoneFlex outdoor AP models:

- ZoneFlex 2741 802.11g Outdoor Access Point
- ZoneFlex 7762 Dual Band 802.11n Outdoor Access Point
- ZoneFlex 7762-S Dual Band 802.11n Outdoor Access Point with Sector Antenna
- ZoneFlex 7762-T Dual Band 802.11n Outdoor Access Point with Omni Antenna
- ZoneFlex 7762-AC Dual Band 802.11n Outdoor Access Point
- ZoneFlex 7762-S-AC Dual Band 802.11n Outdoor Access Point with Sector Antenna
- ZoneFlex 7761-CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem

Part Number 800-70388-001
Published June 2012

www.ruckuswireless.com

Contents

About This Guide

Document Conventions i
Related Documentation ii
Documentation Feedback ii

1 Introducing the ZoneFlex Access Point

Overview of the ZoneFlex Access Point 1
Getting to Know the Access Point Features 2
ZoneFlex 2741 Access Point 3
ZoneFlex 7762 Access Point 7
ZoneFlex 7762-S Access Point 10
ZoneFlex 7762-T Access Point 13
ZoneFlex 7762-AC Access Point 16
ZoneFlex 7762-S-AC Access Point 19
ZoneFlex 7761-CM Cable Modem Access Point 22

2 Connecting an Administrative Computer to a Standalone AP

Configuring the Administrative Computer 27

3 Navigating the Web Interface

Logging In to the ZoneFlex Web Interface 31
Navigating the Web Interface 32
If You Are Using a Dual Band ZoneFlex Access Point 33

4 Configuring the Access Point

Configuring Device Settings 36
Configuring Internet Settings 37
VLAN Settings Overview 38
Configuring NTP Server and Management VLAN 38
Default IP Addressing Behavior 39

Obtaining and Assigning an IP Address 39
Configuring L2TP Connection Settings 42
Configuring Local Subnets 44
Configuring Wireless Settings. 46
Configuring Common Wireless Settings 46
Configuring Wireless # Settings 51
Configuring Ethernet Ports 65
Setting Ethernet Port Type 67
Working with 802.1X on Wired Ethernet Ports 68
Working with Port-Based VLANs 69
Configuring the Hotspot Service 70
Customizing Optional Hotspot Settings 71
Creating a Hotspot Walled Garden 74
Allowing Unrestricted Access by MAC Address 75

5 Managing the Access Point

Viewing Current Device Settings 78
Viewing Current Internet Connection Settings 79
Viewing Current Local Subnet Settings 80
Viewing Current Wireless Settings 81
Viewing Associated Wireless Clients 83
Changing the Administrative Login Settings. 84
Enabling Other Management Access Options 85
Viewing FlexMaster Management Status 88
Pointing the AP to FlexMaster 89
Working with Event Logs and Syslog Servers 90
Enabling Logging and Sending AP Events to a Syslog Server 90
Sending a Copy of the AP Log File to Ruckus Wireless Support 91
Saving Copies of the Current AP Log Files to Your Computer 91
Upgrading the Firmware 93
Upgrading Manually via FTP or TFTP 94
Upgrading Manually via the Web 94
Upgrading Manually via Local File 94
Scheduling Automatic Upgrades 95
Rebooting the Access Point 96
Resetting the Access Point to Factory Defaults. 97

Running Diagnostics 98
Where to Find More Information 100

Index

About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless™ ZoneFlex™ Access Point. This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE: If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

NOTE: Each ZoneFlex Outdoor AP model has its own *Installation Guide* or *Getting Started Guide* that details specific hardware installation procedures for the particular AP model. This guide does not cover installation procedures for these outdoor APs. Refer to the *Installation Guide* or *Getting Started Guide* that shipped with your product for model-specific installation instructions.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at http://support.ruckuswireless.com/

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text Conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
	Information	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
	Warning	Information that alerts you to potential personal injury

Related Documentation

In addition to this guide, each ZoneFlex Access Point documentation set includes the following:

- *Installation Guide/Getting Started Guide*: Provides essential installation and configuration information to help you get the AP up and running within minutes.
- *Online Help*: Provides instructions for performing tasks using the Access Point's Web interface. The online help is accessible from within the Web interface.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

NOTE: If you will be managing your ZoneFlex Access Points using ZoneDirector, refer to the *ZoneDirector User Guide*, available from the Ruckus Wireless website.

Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at docs@ruckuswireless.com

When contacting us, please include the following information:

- Document title
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus Wireless ZoneFlex Outdoor Access Point Release 9.4 User Guide
- Part number: 800-70388-001
- Page 15

1

Introducing the ZoneFlex Access Point

In This Chapter

Overview of the ZoneFlex Access Point 1
Getting to Know the Access Point Features 2

Overview of the ZoneFlex Access Point

Congratulations on your purchase of the Ruckus Wireless ZoneFlex Access Point! ZoneFlex Access Points are the industry's most easy to use, yet robust and feature-rich Wi-Fi Access Points designed to bring power and simplicity together for large-scale outdoor deployments.

Your ZoneFlex Access Point uses BeamFlex™, a patented antenna technology from Ruckus Wireless that allows wireless signals to navigate around interference, extend wireless signal range, and increase speeds and capacity for wireless networks. The BeamFlex antenna system consists of an array of up to fourteen high-gain directional antenna elements that allow ZoneFlex Access Points to find quality signal paths in a changing environment, and sustain the baseline performance required for supporting data, audio and video applications.

Your ZoneFlex Access Point can be deployed in standalone mode or as part of the ZoneFlex Smart WLAN system, in which it can be managed by either FlexMaster or ZoneDirector WLAN controller.

NOTE: For more information on the ZoneFlex system (including FlexMaster and ZoneDirector), BeamFlex, and other Ruckus Wireless technologies, visit www.ruckuswireless.com.

Getting to Know the Access Point Features

This section identifies the physical features of each ZoneFlex Access Point model that is discussed in this guide. Before you begin the installation process, Ruckus Wireless recommends that you become familiar with these features.

- ZoneFlex 2741 Access Point
- ZoneFlex 7762 Access Point
- ZoneFlex 7762-S Access Point
- ZoneFlex 7762-T Access Point
- ZoneFlex 7762-AC Access Point
- ZoneFlex 7762-S-AC Access Point
- ZoneFlex 7761-CM Cable Modem Access Point

NOTE: This guide does not include information on ZoneFlex Indoor Access Points, ZoneFlex 7731 Wireless Bridge, or ZoneFlex 7025 Multimedia Wi-Fi Wall Switch. For information on those ZoneFlex models (along with Ruckus Wireless MediaFlex and MetroFlex product lines), refer to their respective documents available from support.ruckuswireless.com.

ZoneFlex 2741 Access Point

Figure 1 and Figure 2 identify the Access Point external features.

Figure 1. 2471 Access Point LEDs and bottom connectors

Table 3. 2471 LEDs and bottom panel connectors

No	Label	Description
1	LEDs	See "LED Colors and What They Mean" below for more information.
2	RJ45	LAN port that supports Power over Ethernet (PoE) and 10/100Mbps network connections

Table 3. 2471 LEDs and bottom panel connectors

No	Label	Description
3	Reset	Using a pointed object (for example, a pen), press this button to restart the Access Point or to restore it to factory default settings: • To restart the Access Point, press the Reset button once. • To restore the Access Point to factory default, press the Reset button for six (6) seconds. *WARNING: Restoring the Access Point to factory default settings removes all configuration changes that you have made. These include the IP address, password, access control list, and wireless settings. Returning the configuration of these features to their factory default settings may result in network connectivity issues.*
4	12V DC	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point.

LED Colors and What They Mean

Refer to Table 4 below for all possible LED states and what they indicate.

Table 4. 2471 LED states and behaviors

LED	Meaning
OPT	Not used in this model.
DIR	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Flashing green*: The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector.
AIR	• *Green*: The Access Point is functioning as a mesh AP (MAP) and the wireless signal to its uplink MAP is *good* (> 24dBm). • *Fast flashing green (two flashes every second)*: The Access Point is functioning as a mesh AP (MAP) and the wireless signal to its uplink MAP is *poor* (< 24dBm). • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the Access Point cannot find a mesh uplink. • *Off*: The Access Point is operating in standalone mode or, if mesh networking is enabled, the Access Point is functioning as a root AP (RAP).

Table 4. 2471 LED states and behaviors

LED	Meaning
WLAN	• *Green*: The wireless LAN (WLAN) service is up and at least one wireless client is associated with it. If mesh networking is enabled, there are no downlink MAPs connected to this Access Point. • *Fast flashing green (two flashes every second)*: The WLAN service is up and at least one wireless client is associated with it. Mesh networking is enabled and at least one downlink MAP is connected to this Access Point. • *Slow flashing green (one flash every two seconds)*: The WLAN service is up, but no wireless clients are currently associated with it. Mesh networking is enabled and at least one downlink MAP is connected to this Access Point. • *Off*: Either the WLAN is down, or it is up but no wireless clients are currently associated with it. If mesh networking is enabled, there are no downlink MAPs connected to this Access Point.
LAN	• *Green*: The LAN port is connected to a 10/100Mbps device. • *Flashing green*: Traffic is passing through the LAN port. • *Off*: The LAN port is not connected to any network device.
PWR	• *Green*: The Access Point is connected to a power source. • *Off*: No power is available, or the Access Point is not connected to a power source.

If you want to extend the range of your wireless network, you can connect an external high gain antenna to the standard N-type radio frequency (RF) antenna connector on the top panel of the Access Point. The antenna must have a gain of less than 9dBi to comply with FCC and CE regulations.

Figure 2. The 2741 antenna connector is protected by a waterproof antenna connector cover

ZoneFlex 7762 Access Point

Figure 3 and Figure 4 identify the Access Point external features.

Figure 3. 7762 Access Point parts

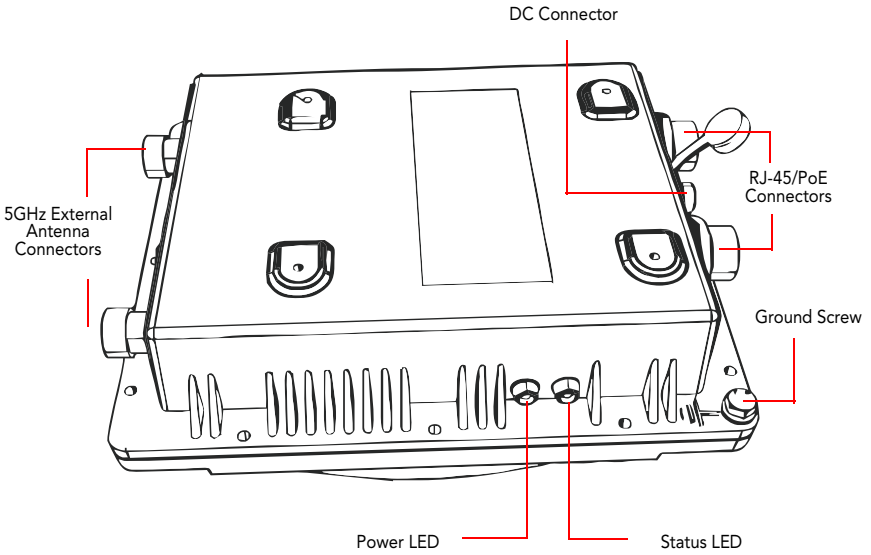


Table 5. LEDs and connectors on the 7762 AP

Label	Description
Power LED	• *Off*: No power is available, or the Access Point is not connected to a power source. • *Red*: The Access Point is powering on. • *Green*: The Access Point is connected to a power source and has completed its power-on sequence.

Table 5. LEDs and connectors on the 7762 AP

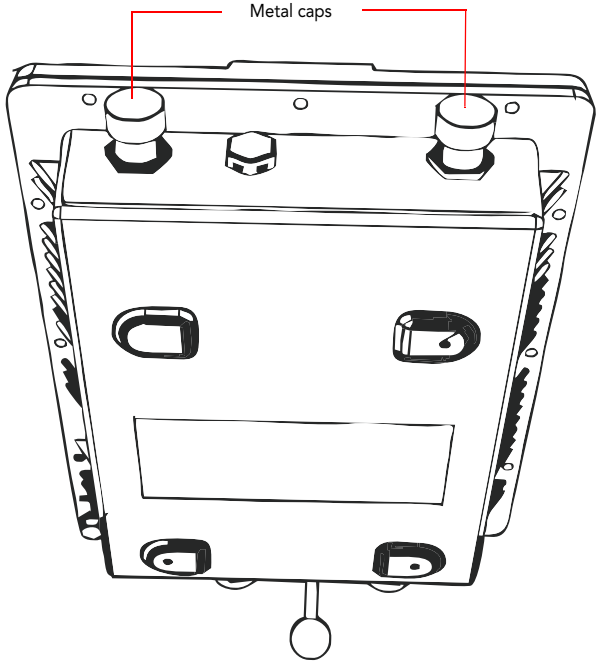
Label	Description
Status LED	If the Access Point is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the Access Point is being managed by Ruckus Wireless ZoneDirector: • *Green*: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green*: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green*: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected). • **PoE OUT** port: Supports 10/100/1000Mbps connections. If the supplied PoE injector is used, this port can supply 802.af PoE to the connected PoE-capable device (for example, another ZoneFlex 7762 AP or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.
DC Connector	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point.

The 7762 includes internal 5GHz antennas, and also provides two external antenna ports, in case you want to attach an external antenna to extend the range of your wireless network.

If you want to use customer-supplied 5GHz external antenna(s), connect the 5GHz external antennas to the standard N-type radio frequency (RF) antenna connectors on the AP.

NOTE: To enable the AP to use the external antennas, select the *Enabled* option in the External Antenna parameter. (This option is disabled by default.)

Figure 4. The 7762 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-S Access Point

Figure 5 shows the Access Point LEDs and connectors, and Table 6 describes them.

Figure 5. 7762-S Access Point LEDs and connectors

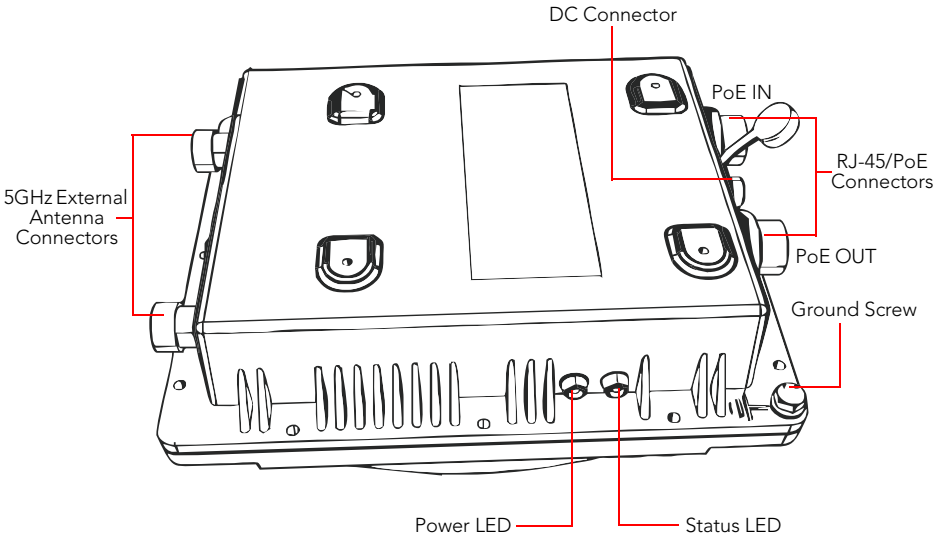


Table 6. LEDs and connectors on the 7762-S Access Point

Label	Description
Power LED	• *Off*: No power is available or the Access Point is not connected to a power source. • *Red*: The Access Point is powering on. • *Green*: The Access Point is connected to a power source and has completed its power-on sequence.

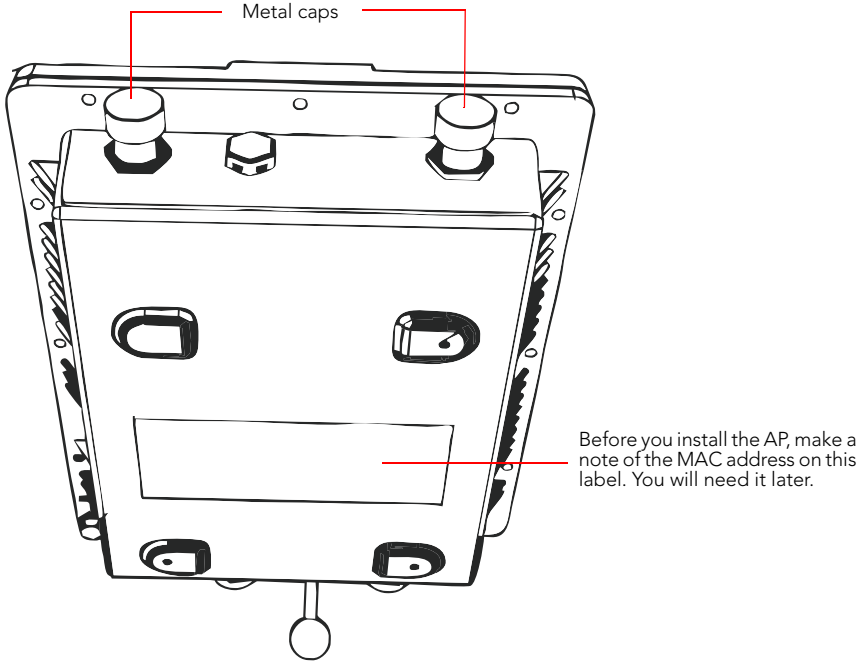
Table 6. LEDs and connectors on the 7762-S Access Point

Label	Description
Status LED	If the Access Point is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the Access Point is being managed by Ruckus Wireless ZoneDirector: • *Green*: The AP is part of a mesh network (either as a Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green*: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with a fair or good signal. • *Slow flashing green*: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected). • **PoE OUT** port: Supports 10/100/1000Mbps connections. If the supplied PoE injector is used, this port can supply 802.af PoE to the connected PoE-capable device (for example, another ZoneFlex 7762-S AP or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.
DC Connector	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point. NOTE: If you connect the Access Point to both PoE and DC power sources at the same time, it will use PoE as the primary power source and DC power as the backup power source.

7762-S 5GHz Antenna Connectors

The 7762-S requires customer-supplied external antenna(s) if you want to use 5GHz or want to use the mesh function. You can connect 5GHz external antennas to the standard N-type radio frequency (RF) antenna connectors on the AP.

Figure 6. The 7762-S 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-T Access Point

Figure 7 and Figure 8 identify the Access Point external features.

Figure 7. 7762-T Access Point parts

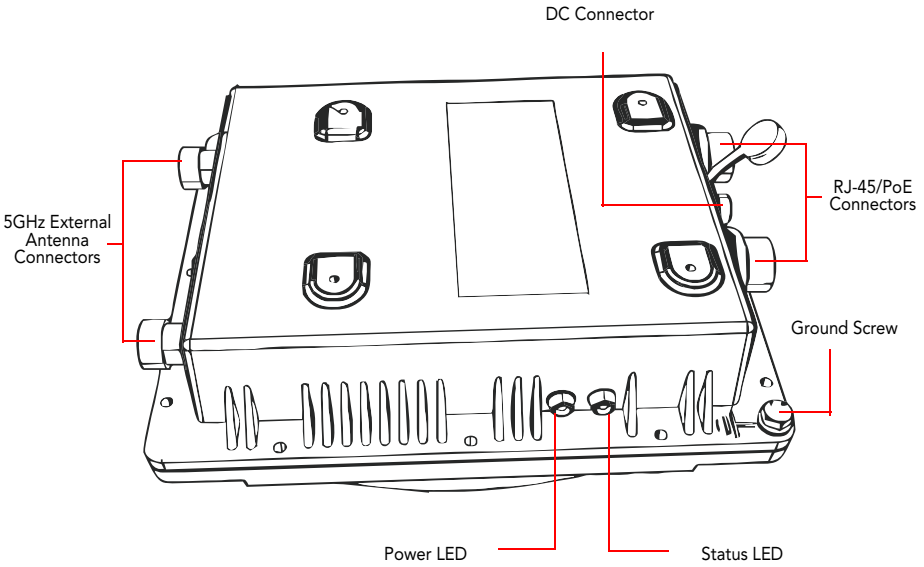


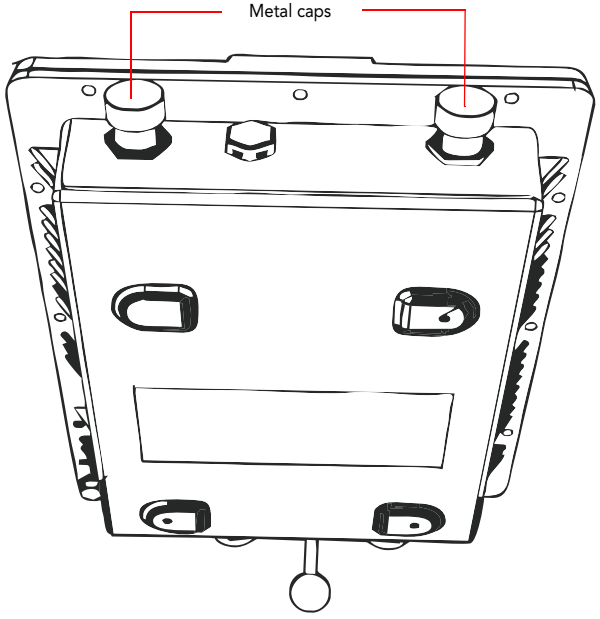
Table 7. LEDs and connectors on the 7762-T AP

Label	Description
Power LED	• *Off*: No power is available, or the Access Point is not connected to a power source. • *Red*: The Access Point is powering on. • *Green*: The Access Point is connected to a power source and has completed its power-on sequence.
Status LED	If the Access Point is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the Access Point is being managed by Ruckus Wireless ZoneDirector: • *Green*: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green*: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green*: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected). • **PoE OUT** port: Supports 10/100/1000Mbps connections. If the supplied PoE injector is used, this port can supply 802.af PoE to the connected PoE-capable device (for example, another ZoneFlex 7762-T AP or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.
DC Connector	In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the Access Point.

The 7762-S requires customer-supplied external antenna(s) if you want to use 5GHz or want to use the mesh function. You can connect 5GHz external antennas to the standard N-type radio frequency (RF) antenna connectors on the AP.

NOTE: The maximum value for the antenna gain that you should set depends on the type of external antennas that you are connecting to the AP.

Figure 8. The 7762-T 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-AC Access Point

Figure 9 and Figure 10 identify the AP external features.

Figure 9. 7762-AC Access Point parts

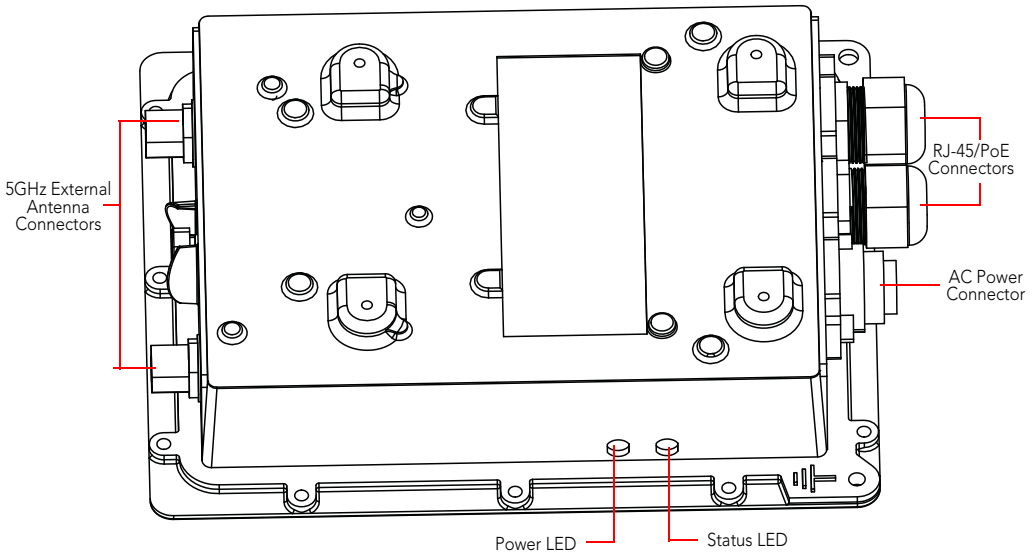


Table 8. LEDs and connectors on the 7762-AC AP

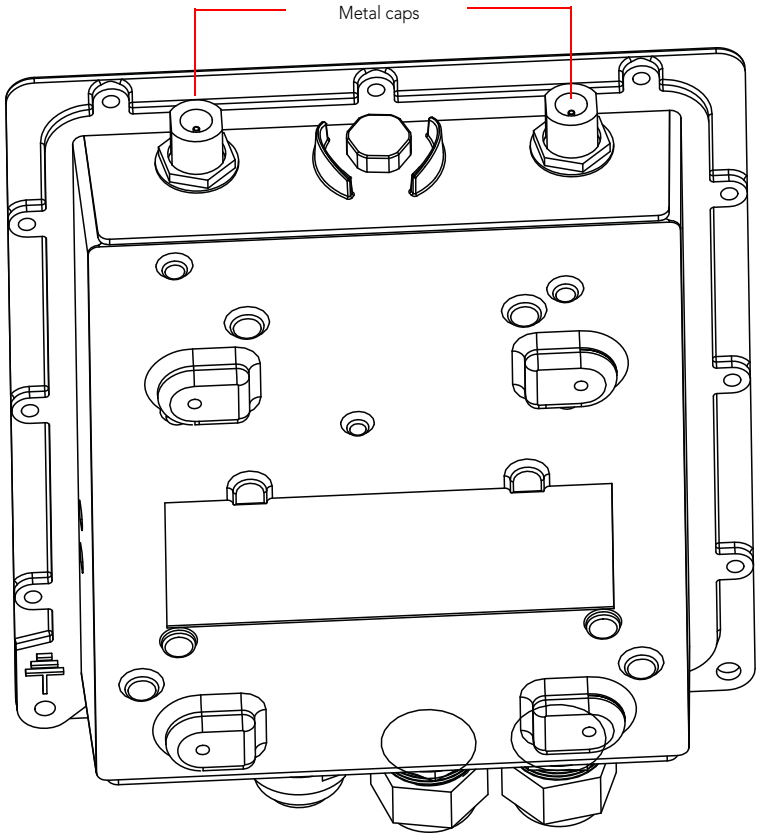
Label	Description
Power LED	• *Off*: No power is available, or the AP is not connected to a power source. • *Red*: The AP is powering on. • *Green*: The AP is connected to a power source and has completed its power-on sequence.

Table 8. LEDs and connectors on the 7762-AC AP

Label	Description
Status LED	If the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the AP is being managed by Ruckus Wireless ZoneDirector: • *Green*: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green*: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green*: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the Ruckus Wireless 60W PoE injector (not supplied, may be ordered separately – part number 902-0180-XX00, where XX is the country code). • **PoE OUT** port: Supports 10/100Mbps connections. If the AP is using AC power or the Ruckus Wireless PoE injector (ordered separately), this port can supply 802.af PoE to the connected PoE-capable device (for example, another ZoneFlex 7762 AC AP or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface. If you use PoE only to power the AP and you want to use the PoE OUT port to supply power to another device, you must use the Ruckus Wireless 60W PoE injector (part number 902-0180-XX00, where XX is the country code), which may be ordered separately.
AC Power Connector	You can use AC to supply power to the AP, in addition to using PoE.

If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 10. The 7762-AC 5GHz antenna connectors are protected by metal caps



ZoneFlex 7762-S-AC Access Point

Figure 11 and Figure 12 identify the AP external features.

Figure 11. 7762-S-AC Access Point parts

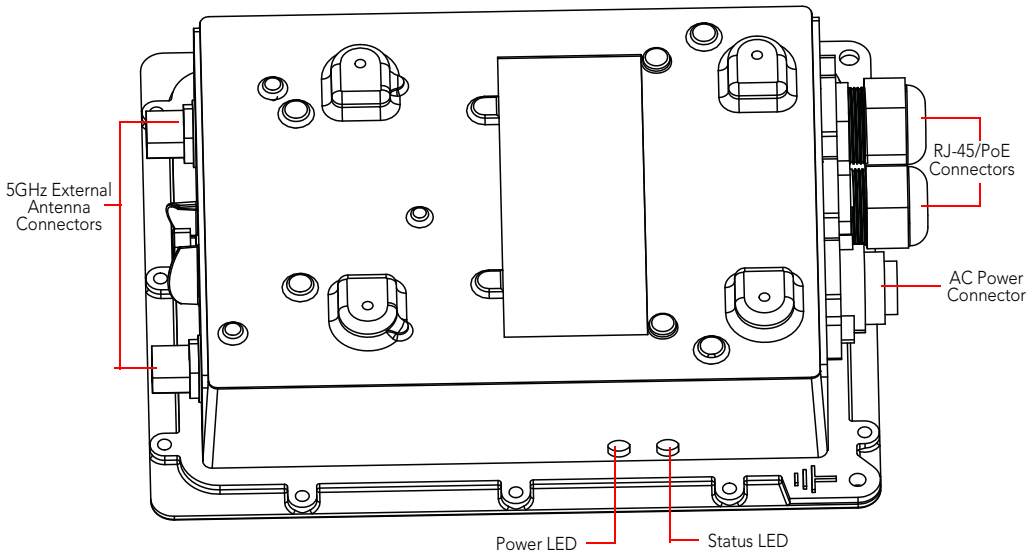


Table 9. LEDs and connectors on the 7762-S-AC AP

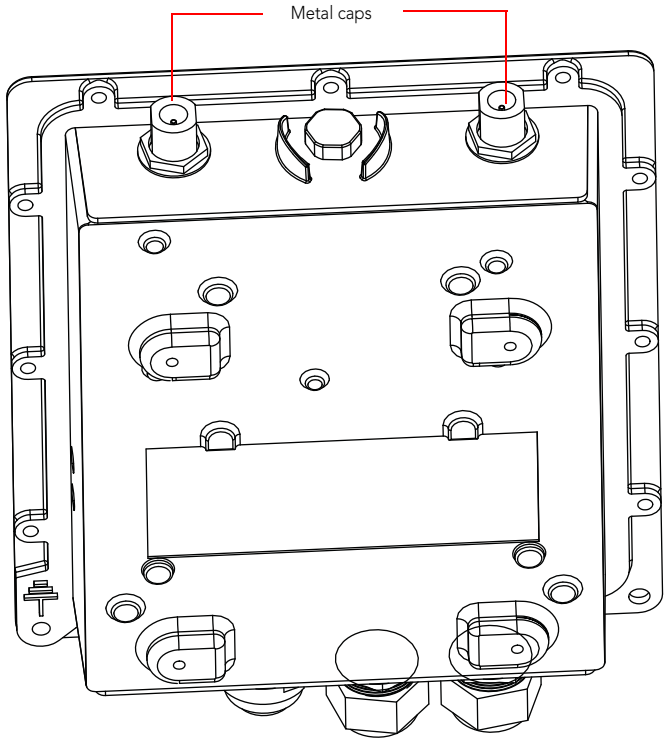
Label	Description
Power LED	• *Off*: No power is available, or the AP is not connected to a power source. • *Red*: The AP is powering on. • *Green*: The AP is connected to a power source and has completed its power-on sequence.

Table 9. LEDs and connectors on the 7762-S-AC AP

Label	Description
Status LED	If the AP is operating in standalone mode: • *Amber*: The WLAN service is up and at least one wireless client is associated with the AP. • *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP. If the AP is being managed by Ruckus Wireless ZoneDirector: • *Green*: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green. • *Fast flashing green*: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal. • *Slow flashing green*: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector. • *Off*: Mesh networking is disabled and the WLAN service is unavailable.
RJ45 Connectors	Two LAN ports that support Power over Ethernet (PoE): • **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the Ruckus Wireless 60W PoE injector (not supplied, may be ordered separately – part number 902-0180-XX00, where XX is the country code). • **PoE OUT** port: Supports 10/100Mbps connections. If the AP is using AC power or the Ruckus Wireless PoE injector (ordered separately), this port can supply 802.af PoE to the connected PoE-capable device (for example, another ZoneFlex 7762 AC AP or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface. If you use PoE only to power the AP and you want to use the PoE OUT port to supply power to another device, you must use the Ruckus Wireless 60W PoE injector (part number 902-0180-XX00, where XX is the country code), which may be ordered separately.
AC Power Connector	You can use AC to supply power to the AP, in addition to using PoE.

If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 12. The 7762-S-AC 5GHz antenna connectors are protected by metal caps



ZoneFlex 7761-CM Cable Modem Access Point

Figure 13 and Figure 14 identify the 7761-CM Cable Modem AP (CMAP) external features.

Figure 13. CMAP parts and connectors (Connector side)

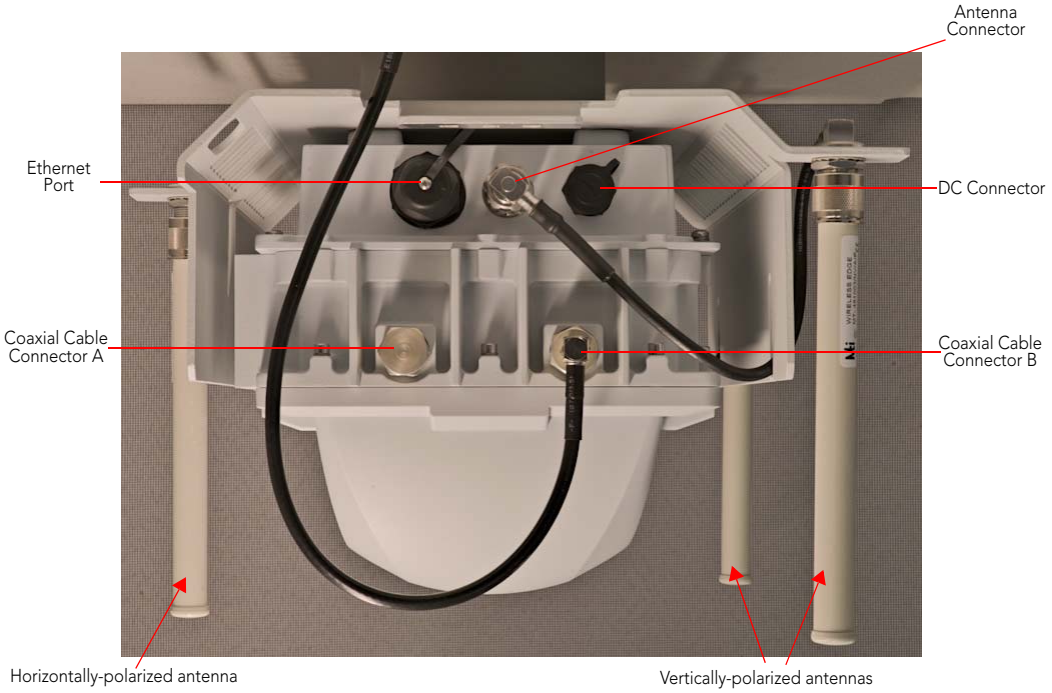


Table 10. Connector-side parts and connectors on the CMAP

Label	Description
Ethernet Port	RJ45 port that supports 10/100Mbps connections and provides Power over Ethernet (PoE) power to compliant devices.
Antenna Connector	One of the three connectors for the three 5GHz antennas supplied with the CMAP. The other two connectors are located on the other side of the unit (see Figure 14).
DC Connector	In addition to the power supplied by the coaxial cable from the CMTS, the CMAP may also be DC powered. Shorting pins 3 and 4 in the DC power connector using an electrical shunt will reset the CMAP to factory default settings.
Coaxial Cable Connector A	Provides a +/-3dB sample of the downstream RF signal as seen by the cable modem. Refer to the ZoneFlex *7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide* for more information on the CMAP signal levels.
Coaxial Cable Connector B	Connects to the cable modem termination system (CMTS) at the headend using a tap on the plant and it provides AC power to the CMAP. AC power is supplied via Power Over Cable (POC).

Figure 14. CMAP parts and connectors (LED side)

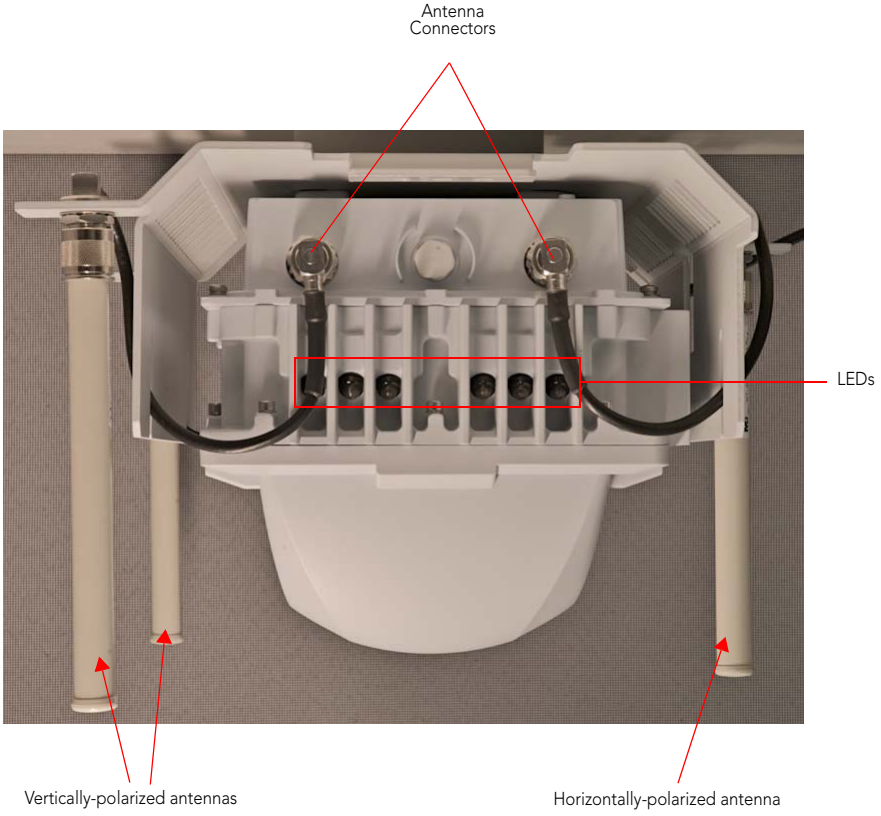


Table 11. LED-side parts and connectors on the CMAP

Label	Description
Antenna Connectors	Two of the three connectors for the 5GHz antennas. The other connector is located on the other side of the unit (see Figure 13).
LEDs	Six LEDs that indicate the status of the CMAP and cable modem. For more information, refer to "LEDs" on page 26.

Connectors

The CMAP provides the following connectors:

- PoE-Out connector: RJ-45 port that can supply power to devices that support PoE.
- Three N-type antenna connectors: Connects to the three 5GHz antennas (not supplied, with the CMAP).
- DC power supply (Ruckus Wireless part number 705-60244-002): Connected through a 4-pin connector, which is normally unused. It may be used to supply DC power to the unit for testing or configuration purposes. The supply has a reset switch that may be used to reset the unit.
- Coaxial cable connectors (see Figure 13): Connector A may be connected to a spectrum analyzer or signal analyzer to allow monitoring of the downstream signal. Connector B must be connected to the CMTS backbone and AC power when deployed in the field.

Ethernet/PoE-Out Port

The CMAP provides one 10/100Mbps RJ45 Ethernet port, which also functions as a PoE-Out port. The PoE-Out port, which can supply up to 15.4 watts (compliant with 802.3af), can be used to power PoE-capable devices (for example, an IP-based surveillance camera).

NOTE: The PoE-Out function is non-operational when the unit is powered via the 12 VDC connector.

NOTE: By default, both Ethernet data and PoE-Out are enabled. If necessary, you can disable PoE-Out from the Web interface.

LEDs

Use the six LEDs to check the status of the Access Point and cable modem. The LEDs behave differently when the Access Point is in standalone mode and when ZoneDirector is managing it. Upon bootup, the LEDs are in *CM (Cable Modem) Mode*. Once bootup is completed, the LEDs alternate between *CM Mode* and *AP Mode*.

Refer to the ZoneFlex *7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide* for more information on the CMAP LED operation.

NOTE: The LEDs also do not indicate whether the AP is in standalone mode or if ZoneDirector is managing the AP. To check if ZoneDirector is managing the Access Point, log into the ZoneDirector Web interface, go to the *Access Points* page, and then search for the Access Point's MAC address. If you are unable to find the Access Point, then it is very likely in standalone mode. If you have multiple ZoneDirectors on the network, make sure you check each one of them.

Supported Power Sources

The CMAP supports the following power sources:

- Power over Cable (POC): 40 to 90 VAC supplied through the RF coaxial cable (attached to Connector B) that is connected to the cable modem termination system (CMTS) backbone. POC is the primary and conventional source of power for the CMAP.
- DC power (via DC connector): External 12 VDC. Use this only when staging or debugging the CMAP.

NOTE: PoE output is disabled when the CMAP is powered via the 12 VDC connector.

Heaters

The CMAP includes two built-in heaters (one for the Access Point and one for the cable modem) that permit operation at extremely low temperatures. They are typically on below 0° C (32° F).

The heaters are enabled by default. If preferred, the Access Point heater can be disabled from the Web interface. The cable modem heater cannot be disabled.

Cable Modem Operation

Refer to the *7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide* for information on the Cable Modem configuration and operation procedures.

2

Connecting an Administrative Computer to a Standalone AP

Ruckus Wireless Access Points can be configured and monitored in standalone mode using an administrative computer. This chapter contains instructions on how to connect an administrative computer to an AP.

NOTE: To administer APs using ZoneDirector (ZD), refer to the *ZoneDirector User Guide*. To administer APs and ZDs using FlexMaster, refer to the *FlexMaster User Guide*.

1. Collect required equipment and information:
   - An administrative computer running Windows 7/Vista/XP/2000 with an Ethernet card installed.
   - Mozilla Firefox 2.0 (or later) or Microsoft Internet Explorer 6.0 (or later) installed on the administrative computer.
   - One Cat5e or better Ethernet cable.
2. Verify that the AP is powered on as described in its associated *Installation Guide*.
3. Continue with Configuring the Administrative Computer.

Configuring the Administrative Computer

NOTE: The following procedure is applicable if the administrative computer is running on Windows XP or Windows 2000. If you are using a different operating system, refer to the documentation that was shipped with your operating system for information on how to modify the computer's IPv4 address settings.

1. On your Windows XP or Windows 2000 computer, open the **Network Connections** (or **Network and Dial-up Connections**) control panel according to how the Start menu is set up:
   - On Windows XP, click **Start** > **Control Panel** > **Network Connections.**
   - On Windows 2000, click **Start** > **Settings** > **Network Connections**.
2. When the Network Connections window appears, right-click the icon for Local Area Connection, and then click **Properties**.

NOTE: Make sure that you configure the Local Area Connection properties, not the Wireless Network Connection properties.

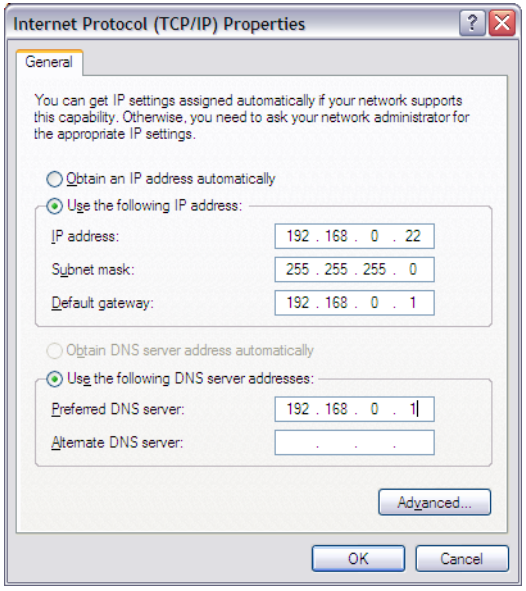
3. When the **Local Area Connection Properties** dialog box appears, select **Internet Protocol (TCP/IP)** from the scrolling list, and then click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box appears.
4. Write down all of the currently active network settings. You will need this information later when you restore your computer to its current network configuration.
5. Click **Use the following IP address**, and then configure the IP address settings with the values listed in Table 12. For a sample configuration, refer to Figure 15.

Table 12. Configure your computer's IP address settings

IP address	**192.168.0.22** (or any address in the 192.168.0.x network – with the exception of **192.168.0.1**, which is already used by the AP)
Subnet mask	**255.255.255.0**
Default gateway	**192.168.0.1**
Preferred DNS server	**192.168.0.1**

You can leave the **Alternate DNS server** box blank.

Figure 15. Sample configuration in the Internet Protocol (TCP/IP) Properties dialog box


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 22
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:
Advanced...
OK
Cancel

6. Click **OK** to save your changes and close the TCP/IP Properties dialog box.
7. Click **OK** again to close the Local Area Connection Properties dialog box.

Windows saves the IP address settings that you have configured. Continue with Connecting the Administrative Computer to the Access Point.

Connecting the Administrative Computer to the Access Point

1. If you are powering the AP with PoE, then continue with Step 2. If you are powering the AP with AC, then continue with Step 5.
2. Connect one end of the Ethernet cable to the Data In port on the PoE injector.
3. Connect the other end of the Ethernet cable to the administrative computer either directly or through a hub.
4. You have completed connecting the administrative computer to the AP. Continue with Chapter 3.
5. Connect one end of the Ethernet cable to the **PoE IN** port on the AP.
6. Connect the other end of the Ethernet cable to the administrative computer.
7. You have completed connecting the administrative computer to the AP. Continue with Chapter 3.

3

Navigating the Web Interface

In This Chapter

Logging In to the ZoneFlex Web Interface 31
Navigating the Web Interface 32

Logging In to the ZoneFlex Web Interface

If you need to manage your AP, you do it with the features of the ZoneFlex Web interface (which you already used to set up the AP for use).

If your ZoneFlex network will be managed by a Ruckus Wireless ZoneDirector, you can manage APs through ZoneDirector rather than individually logging in to each AP's Web interface.

NOTE: The following procedure assumes that you know the static IP address of the AP (now in use), or you have some means of determining the dynamic IP address in use by the AP. The PC you use for AP administration should be on the management VLAN, if VLANs are used in your network.

To log into the Web interface

1. On the PC, open a Web browser window.
2. In the address or location bar, type the IP address of the AP. Default IP address for standalone ZoneFlex APs:

   `192.168.0.1`
3. Press <Enter> to connect to the Web interface.
4. If a Windows security alert dialog box appears, click **OK**/**Yes** to proceed. The Ruckus Wireless Admin login page appears.
5. In **Username**, type `super`.
6. In **Password**, type `sp-admin`.
7. Click **Login**.

The ZoneFlex Access Point Web interface appears.

Navigating the Web Interface

You manage the Access Point through a Web browser-based interface that you can access from any networked computer. Table 13 lists the Web interface features that are identified in Figure 16.

Figure 16. Elements of the ZoneFlex AP Web Interface

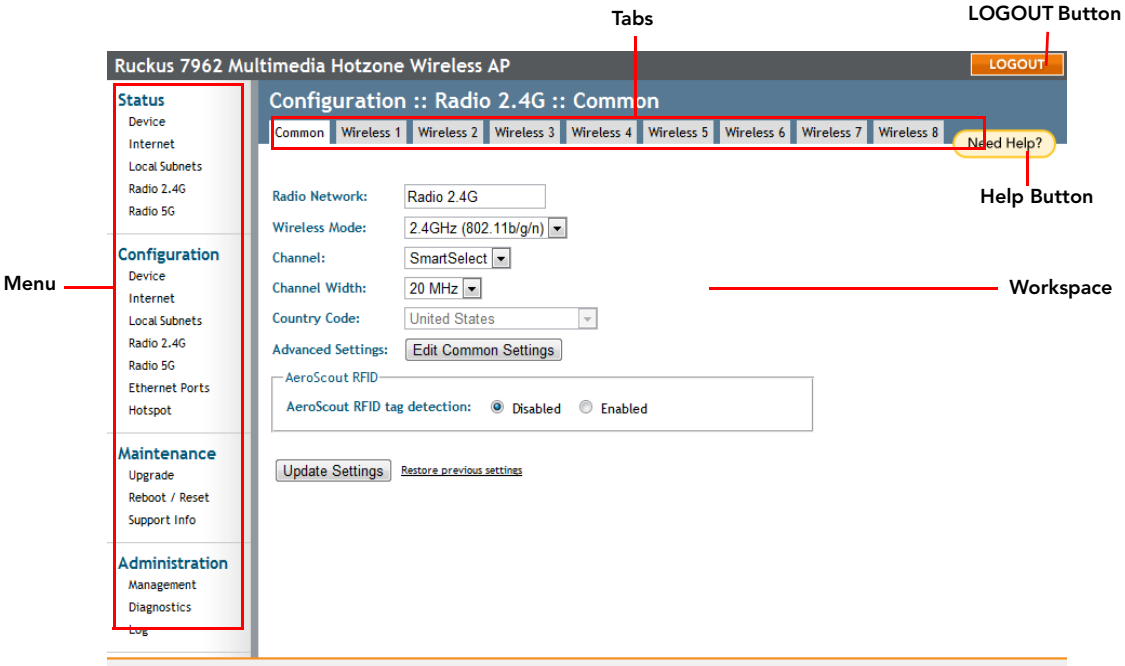


Table 13. ZoneFlex AP Web interface elements

Element	Description
Menu	Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.
Tabs	Contains additional options for the configuration page. For example, the **Configuration** > **Wireless** page includes one tab for common wireless configuration and eight tabs for each of the available WLANs.
Workspace	This large area displays features, options and indicators relevant to your menu bar choices.
Logout Button	Click this button to log out of the AP.
Help Button	Click this button to open a help window with information related specifically to the options currently displayed in the workspace.

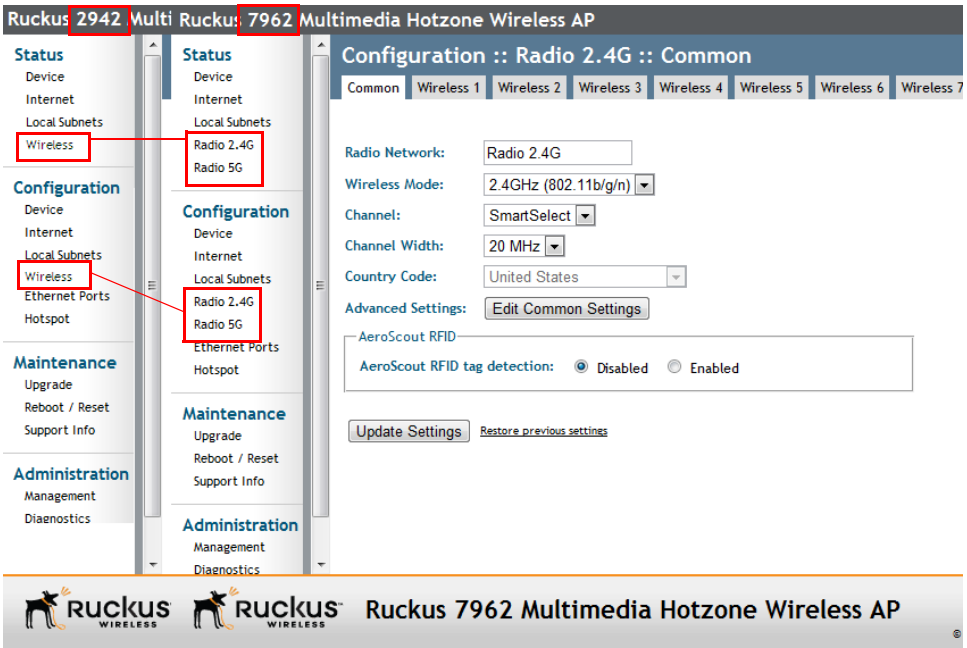
If You Are Using a Dual Band ZoneFlex Access Point

When your ZoneFlex AP model is dual band (all outdoor APs other than ZF 2741), note that elements on the Web interface menu are slightly different from the other (single band) ZoneFlex AP models.

Dual band ZoneFlex APs have one 2.4GHz radio (for 802.11b/g/n clients) and one 5GHz radio (for 802.11a/n clients). The wireless settings for these two radios need to be configured separately, which is why the dual band AP Web interface has the **Radio 2.4G** and **Radio 5G** menu items, instead of a single **Wireless** menu item in other models.

Figure 17 highlights the differences between single band and dual band ZoneFlex AP menus.

Figure 17. Menu items are slightly different in single band APs (left) and dual band ZoneFlex AP models (right)



4

Configuring the Access Point

In This Chapter

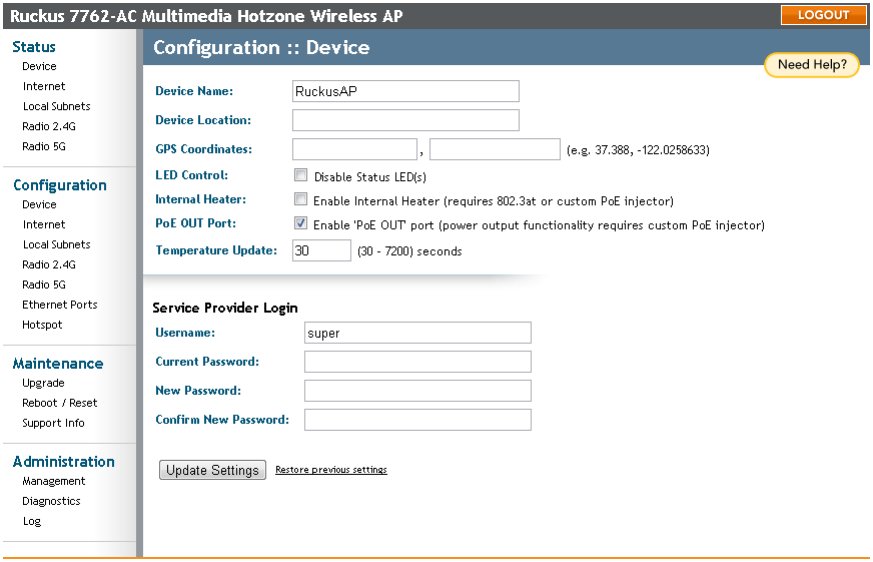
Configuring Device Settings 36
Configuring Internet Settings 37
Configuring Local Subnets 44
Configuring Wireless Settings 46
Configuring Ethernet Ports 65
Configuring the Hotspot Service 70

This chapter provides instructions for configuring ZoneFlex Access Points in a stand-alone configuration. If you will be managing your ZoneFlex network using ZoneDirector refer to the *ZoneDirector User Manual*, available in PDF format from the Ruckus website, at http://support.ruckuswireless.com/documents.

Configuring Device Settings

Device settings refer to the device name, temperature update, location and service provider login settings. (Temperature update is only available on certain ZoneFlex models.)

Figure 18. The Configuration > Device page



To configure the device settings

1. Go to **Configuration** > **Device**. The Configuration > Device page appears.
2. In **Device Name**, type a new name for the AP or leave as is to accept the default AP name (`RuckusAP`). The device name identifies the Access Point among other devices on the network.
3. Configure the following optional settings as desired:
   - Enter **Device Location** and **GPS Coordinates** to keep track of the physical location of the AP.
   - Check the box next to **Disable status LEDs** under **LED Control** (specific models only) to disable the status LEDs. This can be useful if the AP is installed in a public location to avoid drawing attention to the AP.
   - Enable **Internal Heater** and **PoE OUT Port** (specific models only) if needed.
   - In **Temperature Update** (specific models only), enter the interval (in seconds) to record the internal temperature of the AP.
4. Under **Service Provider Login**, change the login information as required:
   - **Username**: Type the name that you want to use for logging in to the Web interface. The default user name is `super`.

- **Current Password**: When you are entering a New Password, type the new existing password. The default password is `sp-admin`.
- **New Password**: Type the new password that you want to use. The password must consist of six to 32 alphanumeric characters only.
- **Confirm New Password**: Retype the new password to confirm.

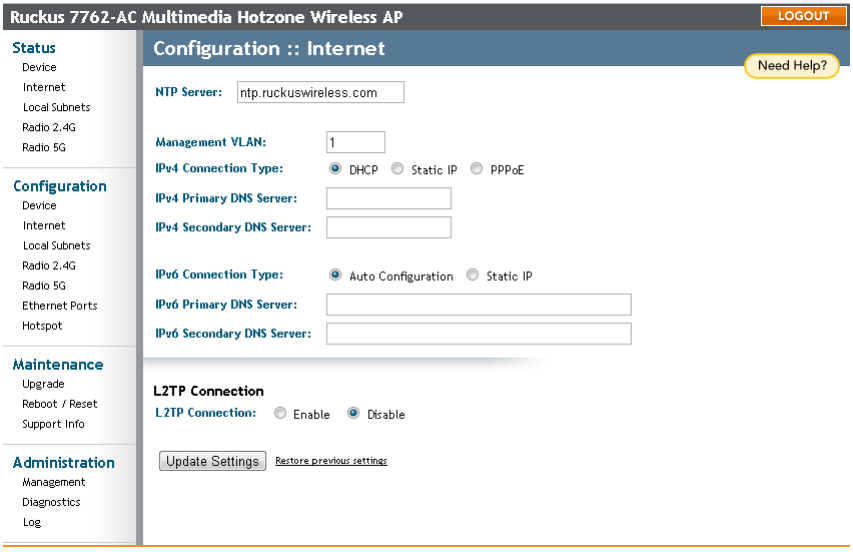
5. Click **Update Settings** to save and apply your changes.

Configuring Internet Settings

Internet settings define how the Access Point connects to your local area network and to the Internet. This section describes how to view and configure the Access Point's Internet settings. Topics discussed include:

- VLAN Settings Overview
- Configuring NTP Server and Management VLAN
- Default IP Addressing Behavior
- Obtaining and Assigning an IP Address
- Configuring L2TP Connection Settings

Figure 19. The Configuration > Internet page



VLAN Settings Overview

A Ruckus Wireless Access Point is essentially a network switch with the capability to service Wi-Fi connections. As such, like many advanced switches, Ruckus APs conform to the IEEE 802.1Q standard -- the standard that defines virtual LANs. In an 802.1Q switch, the concept of VLANs is always present. If a packet arrives without an 802.1Q header, it is assigned to the "native VLAN" or "untag VLAN."

Each of the AP's wireless interfaces can be assigned a single VLAN. When a packet enters the AP through its wireless interface, the packet is assigned to the Access VLAN configured on the Configuration > Wireless page (by default, 1).

AP Ethernet ports however, can be configured to pass all VLAN traffic (Trunk Ports) or multiple specific VLANs (General ports).

The VLAN displayed in the Web interface shows the AP's view of the VLAN environment; when a packet arrives at an AP's Ethernet port, the port's VLAN configuration helps determine if the packet is accepted or not (VLAN membership), and assign a default VLAN (untagged VLAN) if the packet contains no 802.1Q header.

In general, if your network has VLANs deployed already, you should apply VLAN configuration to Ruckus APs so that the configuration across the network is consistent.

Configuring NTP Server and Management VLAN

- NTP Server
- Management VLAN

NTP Server

A Network Time Protocol (NTP) server should be configured to ensure that the Access Point maintains the correct time. The default Ruckus Wireless NTP server (ntp.ruckus-wireless.com) can be used if you do not have an NTP server on your network.

If you want the AP to contact a different NTP server, you can do so by going to **Configuration > Internet** and entering the host name in **NTP Server** at the top of the page.

Management VLAN

CAUTION: Changing the Management VLAN will cause you to be immediately disconnected from the Web interface if the computer you are using is not on the same VLAN. Do not change the Management VLAN unless your admin PC is on the same VLAN, or you will be disconnected and unable to connect again without factory resetting the AP.

If you want to place this AP's management traffic into a management VLAN, enter the VLAN ID in the **Management VLAN** field and click **Update Settings**.

Default IP Addressing Behavior

By default, the Access Point is configured to automatically obtain an IPv4 address from a DHCP server on the network. If the Access Point does not detect a DHCP server, it automatically assigns itself the static IP address `192.168.0.1` to make it easier for you to preconfigure and deploy it on your network.

For IPv6, the Auto Configuration setting serves the same purpose as DHCP. The default static IPv6 address is `fc00::1`.

Obtaining and Assigning an IP Address

There are three methods of assigning IP addresses to the Access Point:

- DHCP / Auto Configuration
- Static IP
- PPPoE

DHCP / Auto Configuration

If you leave the Access Point at its default configuration, it will attempt to obtain an IPv4 address from a DHCP server on the network.

In an IPv6 network environment, the AP will attempt to obtain an IPv6 address from an IPv6 Auto Configuration server.

Renewing and Releasing DHCP

This task should be performed only if you have access to the DHCP server or have some way to determine what IP address has been assigned to the AP. It serves as a troubleshooting technique when IP addresses to one or more networked devices prove to be unusable or in conflict with others, or when the AP loses its DHCP-assigned IP address for some reason.

Figure 20. Renew or Release DHCP

To renew or release the DHCP server-assigned IP address

1. Go to **Status** > **Internet**.
2. Review the current settings.
3. If the current **Connection Type** is **DHCP**, you will be able to see the currently-assigned IP address and subnet mask listed below.
   - To force the AP to release its DHCP-assigned IP address, click **Release DHCP**. This will disconnect the user from Web interface as the system reverts to its default IP address. Log in to the AP using the default IP address (192.168.0.1) and click on **Renew DHCP** to request a new lease from the DHCP server.
   - Click **Renew DHCP** to request a new IP address lease from the DHCP server. *Note: The IP address may or may not change depending on the lease time offered to this AP.*
4. Click **Update Settings** to save your settings.

Static IP

There are at least two instances when you would want to configure a static IP address for the Access Point:

- If the current IP address that the Access Point is using consistently conflicts with that of another AP on the network.
- If you want to switch from DHCP to static IP addressing, for use in managing or maintaining the Access Point.

Unless you are able to determine the IP address assigned by the DHCP/Auto Configuration server to the Access Point, it may prove helpful for anyone needing administrative access to assign a static IP address.

To assign a static IP address to the AP

1. Go to **Configuration** > **Internet**. The *Configuration > Internet* page appears.
2. You can configure static addresses for IPv4, IPv6 or both. The AP will maintain both sets of IP address settings if both are configured.
3. In *IPv4 Connection Type* or *IPv6 Connection Type*, select **Static IP**.
4. When the *Internet Connection Settings* options appear, you can make changes to the following settings:
   - **Primary DNS Server**: The IP address of the primary Domain Name System (DNS) server.
   - **Secondary DNS Server**: The IP address of the secondary Domain Name System (DNS) server.
   - **IPv4/IPv6 Address**: Enter the static IP address that you want to assign to the AP in either IPv4 (dot-decimal) or IPv6 (colon-separated) format.
   - **Subnet Mask (IPv4)/Prefix Length (IPv6)**: Enter the subnet mask or prefix length for the network.
   - **Gateway**: Enter the gateway IP address of the Internet interface.
5. Click **Update Settings** to save your changes.

PPPoE

Point to Point Protocol over Ethernet (PPPoE) is a Layer 2 protocol which uses the PPP (Point to Point) protocol to connect a client system to a server system over a one to one network link. All traffic for a PPPoE connected client must go through the PPPoE server to reach the client. A PPPoE server can therefore be used to route, NAT, firewall, and perform QoS traffic shaping.

If a PPPoE server is used to distribute Internet access to subscribers, the Access Point can be configured with a PPPoE username and password to authenticate with the PPPoE server.

PPPoE is available only for the IPv4 connection type; PPPoE is not supported in IPv6 environments.

To set the IPv4 connection type to PPPoE

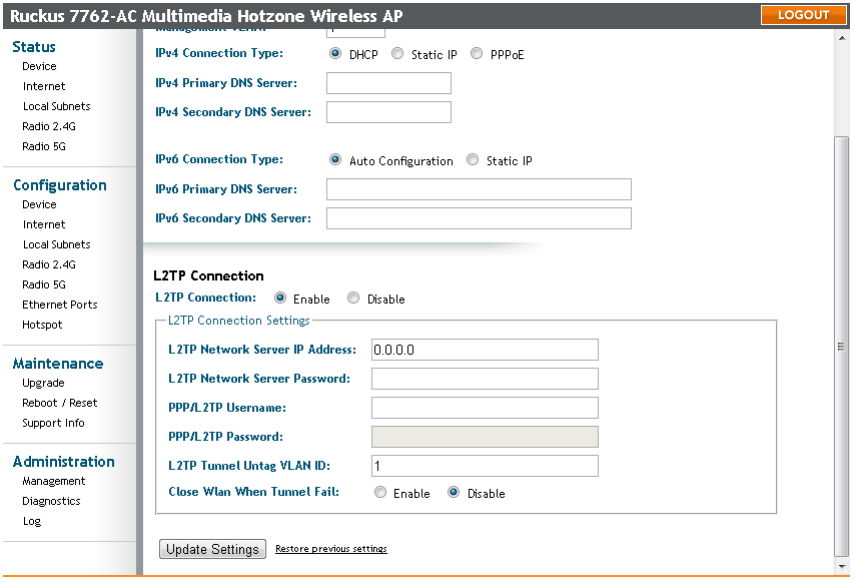
1. Go to **Configuration > Internet**.
2. Under *IPv4 Connection Type*, select **PPPoE**.
3. Enter an **IPv4 Primary DNS Server** address. *Secondary DNS Server* is optional.
4. Enter a **PPPoE Username**.
5. Enter a **PPPoE Password**.
6. Retype the password in **PPPoE Password Confirmation**.
7. Click **Update Settings** to save your changes.

Configuring L2TP Connection Settings

You can implement transparent bridging with ZoneFlex through the use of L2TP (Layer 2 Tunneling Protocol) tunneling. By tunneling traffic from a ZoneFlex AP to a centralized data center, access controllers with policy enforcement software can apply rules and services. In a typical WLAN implementation, these rules include a captive portal to authenticate users' credentials.

In the case of L2TP, the ZoneFlex AP functions as a remote bridge. As such, it forwards traffic into PPP sessions over the L2TP tunnel. This implementation ensures that you have complete visibility into MAC addresses of users, as individual Wi-Fi clients are essentially placed (bridged) onto the ISP's core network.

Figure 21. L2TP Connection



To configure L2TP tunneling

1. Go to **Configuration** > **Internet**.
2. Under **L2TP Connection**, click **Enable**.
3. In **L2TP Network Server IP Address**, type the IP address of the L2TP network server (LNS) to which the device will connect.
4. In **L2TP Network Server Password**, type the L2TP server password.
5. If your network requires PPP authentication, configure the following fields under L2TP/PPP Authentication:
   - **Username**: Type your appropriate PPP user name.
   - **Password**: Type the password appropriate to the account.
   - **L2TP Tunnel Untag VLAN ID**: Enter the Untag VLAN ID for the L2TP tunnel.
6. In **Close WLAN When Tunnel Fail**, select **Enable** if you want to disable the WLAN when the tunnel connection is lost. This prevents clients from remaining seemingly connected to the WLAN but without Internet connectivity.
7. Click **Update Settings** to save your settings.

Configuring Local Subnets

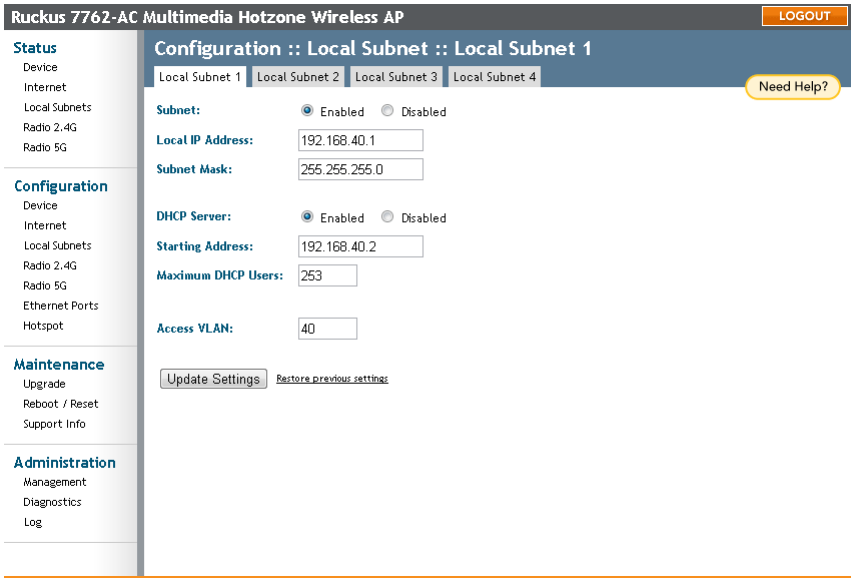
ZoneFlex Access Points can be configured to provide routing/network address translation (NAT) functionality by using the Local Subnets feature. When a Local Subnet is enabled, the standalone AP plays the role of a gateway router with the ability to manage its own subnets, providing DHCP server and DNS cache functions for both wired and wireless clients. These clients can be assigned private IP addresses from a user-defined address pool. Traffic from the client station in private address space appears on the outside as if generated by the AP itself. In this way, the AP performs Layer 3 packet forwarding not only for Hotspot/WISPr usage, but for standard usage as well.

Up to four IP subnets can be configured per AP, each with its own VLAN and address range which cannot conflict with one other.

To configure a local subnet for router mode support

1. Go to **Configuration > Local Subnets**. The four tabs at the top (*Local Subnet 1 - Local Subnet 4*) allow you to configure each of the four subnets independently.
2. Click **Enabled** next to **Subnet**. The local subnet configuration options appear.
3. In **Local IP Address**, enter an IP address for the gateway. The default address for Subnet 1 is `192.168.40.1`. This address can be used to access the AP's Web interface for configuration and monitoring from devices connected to this subnet.
4. In **Subnet Mask**, typically you would want to leave the setting at its default value (`255.255.255.0`) for a Class C subnet with an address pool of up to 254 addresses. An error appears if you enter an invalid IP/netmask combination.
5. In **DHCP Server**, click **Enabled** if you want to enable DHCP for this subnet. Starting Address and Maximum DHCP Users fields appear.
6. In **Starting Address**, enter an address in the same subnet as the Local IP Address (e.g., **`192.168.40.2`**).
7. In **Maximum DHCP Users**, enter the maximum number of clients that can be assigned addresses by DHCP in this subnet (valid values are 1-253 if the default subnet mask is used).
8. In **Access VLAN**, enter a VLAN ID to segment client traffic arriving from this subnet from other network traffic. (Example: if you use the default 192.168.40.1 address range, you would generally want to use "40" as the VLAN for this subnet.)
9. Click **Update Settings** to save your changes. The local subnet is created immediately and can now be applied to WLANs or Ethernet ports from their respective configuration pages.

Figure 22. Configuring local subnets and enabling router mode



Configuring Wireless Settings

This section describes how to configure the wireless settings of the Access Point. There are two types of wireless settings that you need to configure:

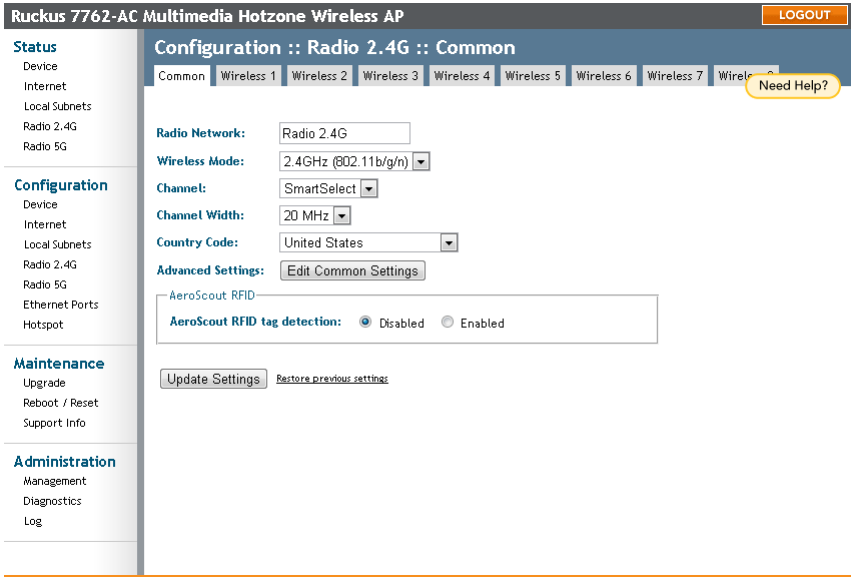
- Configuring Common Wireless Settings: Includes the wireless mode, country code, and advanced wireless settings, such as the wireless transmit power and wireless protection mode. These settings are applied to all WLANs.
- Configuring Wireless # Settings: The Wireless # tabs ("Wireless 1" through "Wireless 8" on the 2.4GHz radio and "Wireless 9" through "Wireless 16" on the 5GHz radio) provide settings for customizing each WLAN individually.

Refer to the sections below for instructions on how to configure each set of wireless settings.

Configuring Common Wireless Settings

Common wireless settings are settings that are applied to all WLANs. On single radio APs, go to **Configuration > Wireless**. On dual radio APs, you configure these settings for the 2.4GHz and 5GHz radios independently by going to **Configuration > Radio 2.4G** or **Configuration > Radio 5G**.

Figure 23. The Configuration > Wireless > Common page



To configure the wireless settings common to all WLANs

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Make changes to the common wireless settings listed in the table below.

Setting	Description
Radio Network	(Dual radio APs only) Allows you to change the name of the 2.4GHz and 5GHz radios (default: "Radio 2.4G" and "Radio 5G").
Wireless Mode	**On 802.11b/g APs:** The wireless mode options include the following: • *Auto-Select*: Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting. • *2.4GHz 54 Mbps (For faster 802.11g devices only)*: Allows only 802.11g-compliant devices to join the network. • *2.4GHz 11Mbps (For slower 802.11b devices only)*: Allows only 802.11b-compliant devices to join the network. **On dual radio 802.11n APs:** On dual radio 802.11n APs, the wireless mode is determined by radio; i.e., for the 2.4GHz radio, the mode is set to 2.4GHz (802.11b/g/n), while for the 5GHz radio, the mode is set to 5GHz (802.11a/n).
Channel	This option lets you select the channel used by the network. You can choose **SmartSelect**, or choose one of a specific number of channels. If you choose **SmartSelect**, the AP automatically selects the best channel (encountering the least interference) to transmit the signal.
Channel Width (11n APs only)	On 802.11n Access Points, the option to choose 40MHz channel width provides (theoretically) double the data capacity of the channel. However, wider channel width means fewer channels available, and more interference with other wireless signals.

Country Code	This option (if enabled) lets you select your country or region code.
Advanced Settings	Refer to "Reviewing Common Advanced Settings" on page 49.
AeroScout RFID	Select **Enabled** to enable AeroScout RFID tag detection.
External Antenna	*NOTE: This option only appears if you are using the ZoneFlex 2942 AP.* The ZoneFlex 2942 AP provides an external antenna port, in case you want to attach an external antenna to extend the range of your wireless network. To enable the AP to use the external antenna, select the **Enabled** option in this section. This option is disabled by default.

CAUTION: Selecting the incorrect country or region may result in violation of applicable laws. If you purchased the Access Point in the United States, you do not need to set the country code manually. Ruckus Wireless devices that are sold in the US are preconfigured with the correct country code and this setting is non-configurable.

3. If you are using AeroScout Tags in your organization to locate assets or personnel, you can use your ZoneFlex AP to relay location or presence data from the AeroScout Tags to the AeroScout Engine via Wi-Fi.

   To enable the AP to relay AeroScout data, click the **Enabled** option in **AeroScout-RFID tag detection**.

   To check the status of the AeroScout communication agent (which relays location data from AeroScout Tags to the AeroScout Engine), go to the **Status > Wireless** page. Refer to "Viewing Current Wireless Settings" on page 81 for more information.

NOTE: For other AeroScout-related configuration, refer to the AeroScout documentation that was shipped with your AeroScout Tag and AeroScout Engine.

NOTE: If ZoneDirector exists on the network, you can enable AeroScout RFID tag detection on all its managed APs at once. Refer to the ZoneDirector online help for more information.

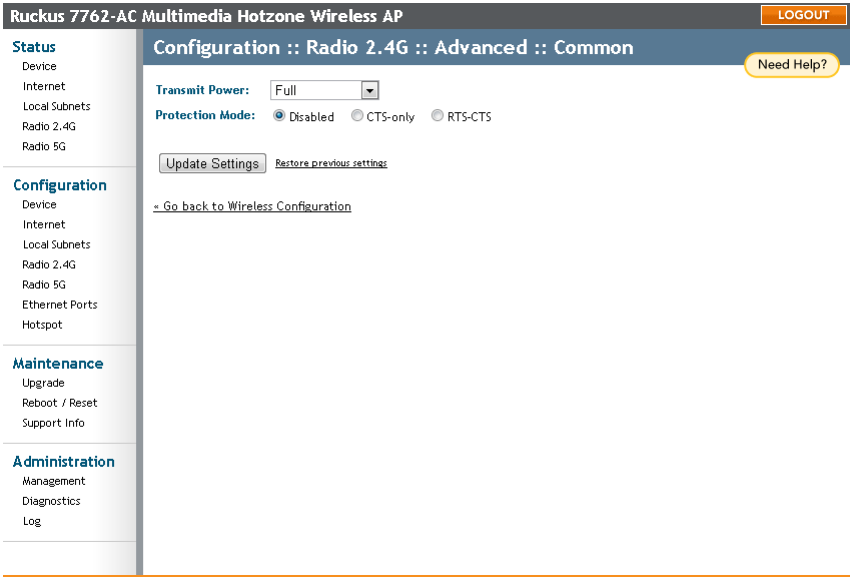
4. Click **Update Settings** to save your settings.

Reviewing Common Advanced Settings

Advanced wireless settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings be retained for best performance.

CAUTION: To fully benefit from the Access Point's capabilities, it is advisable not to change these values unless absolutely necessary.

Figure 24. The Configuration > Wireless > Advanced > Common page



To configure the advanced common options

1. On the **Configuration** > **Wireless** page, click **Edit Common Settings**. The *Configuration > Wireless > Advanced > Common* page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G > Edit Common Settings**.

2. Configure the advanced settings listed in Table 14 as required.

Table 14. Advanced wireless common settings

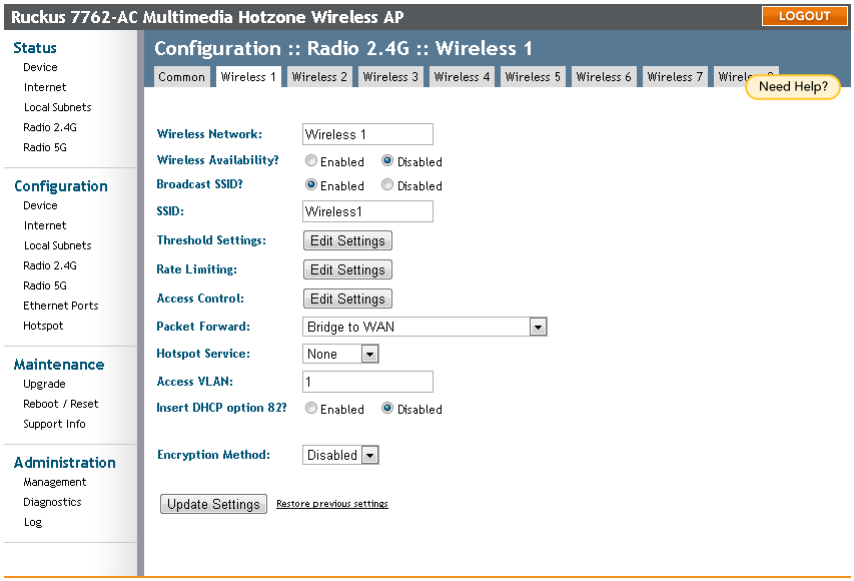
Option	Description
Transmit Power	The default setting is **Full**. Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the predefined power (this value differs according to the current country code).
Protection Mode	(Disabled by default.) If you activate protection, you control how 802.11 devices know when they should communicate with another device. This is important in a mixed environment of both 802.11b and 802.11g/11n clients. *WARNING: Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g/11n devices but will severely decrease performance.* • **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification. • **RTS/CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.

3. Click **Update Settings** to save and apply the changes.

Configuring Wireless # Settings

The Access Point provides up to eight wireless LANs per radio that can be individually configured to provide different kinds of services for different kinds of wireless clients, traffic types or different user groups. Each WLAN can be configured with separate security settings, VLANs, access controls and rate limiting policies, among other settings.

Figure 25. Wireless # settings



To configure wireless # settings

1. Go to **Configuration** > **Wireless**. The *Configuration > Wireless > Common* page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click one of the eight **Wireless (#)** tabs. The *Configuration > Wireless > Wireless [#]* page appears.
3. Review the WLAN options listed in Table 15, and then make changes as required.

Table 15. WLAN options

Option	Description
Wireless Network	This wireless network name is for management purposes only, and is not visible to the user.

Wireless Availability	This option controls whether or not the wireless network is available to users (Enabled or Disabled).
Broadcast SSID	This option controls whether or not the WLAN SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user to be told the correct SSID before they can connect to your network.
SSID	This is the publicly-broadcast "name" of your wireless network. SSIDs can contain up to 32 alphanumeric characters and are case-sensitive. The maximum SSID length can only contain between 2 and 32 characters, including characters from ! (char 33) to ~ (char 126).
Threshold Settings	This button opens a page where you can configure the Protection Mode you activated on the *Configuration > Wireless > Advanced > Wireless [#]* page. If Protection Mode is not active, ignore this option. For more information, see "Setting Threshold Options" on page 60.
Rate Limiting	This button opens a page where you can configure upload and download limits per station. For more information, see "Rate Limiting" on page 61.
Access Control	This button opens a page where you can configure access controls for the WLAN. For more information, see "Controlling Access to the Wireless Network" on page 62.
Packet Forward	**Isolated**: Selecting Isolated causes the traffic from this WLAN to terminate at the Access Point. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this WLAN to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of wireless packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
Hotspot Service	Select a Hotspot configuration from the list to enable Hotspot service on this WLAN, if you have configured it from the Configuration > Hotspot page. See "Configuring the Hotspot Service" on page 70.
Local Subnet	This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forwarding*, and allows you to choose which subnet this WLAN's traffic will be part of. You must have previously configured a subnet from the *Configuration > Local Subnets* page before it becomes available here.

Access VLAN	Enter a VLAN ID to segment all traffic arriving from this WLAN to a specified VLAN. Default is 1.
Dynamic VLAN	This setting is available only with WPA encryption and 802.1X authentication. Dynamic VLAN allows the dynamic assignment of VLANs to clients based on RADIUS attributes. Enable this option only if your RADIUS server is configured to segment clients using dynamic VLAN.
Insert DHCP option 82	When this option is enabled on an SSID, additional information will be encapsulated in DHCP option 82 and inserted into DHCP request packets. Current format of option 82 is: `Circuit ID sub-option: WLAN:<IFNAME>:<VLAN>:<SSID>:<MODEL>: <HOSTNAME>:<DEVMAC>` This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.
Encryption Method	By default, all data exchanges on your wireless network are not encrypted, but you can select an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption settings. *Ruckus Wireless strongly recommends using WPA as the encryption method as WEP has been proven to be easily circumvented.* For more information, see either "Using WEP" on page 54 or "Using WPA" on page 56.

4. When you are finished, click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.
5. Click **Go back to Wireless Configuration** to reopen the previous page.

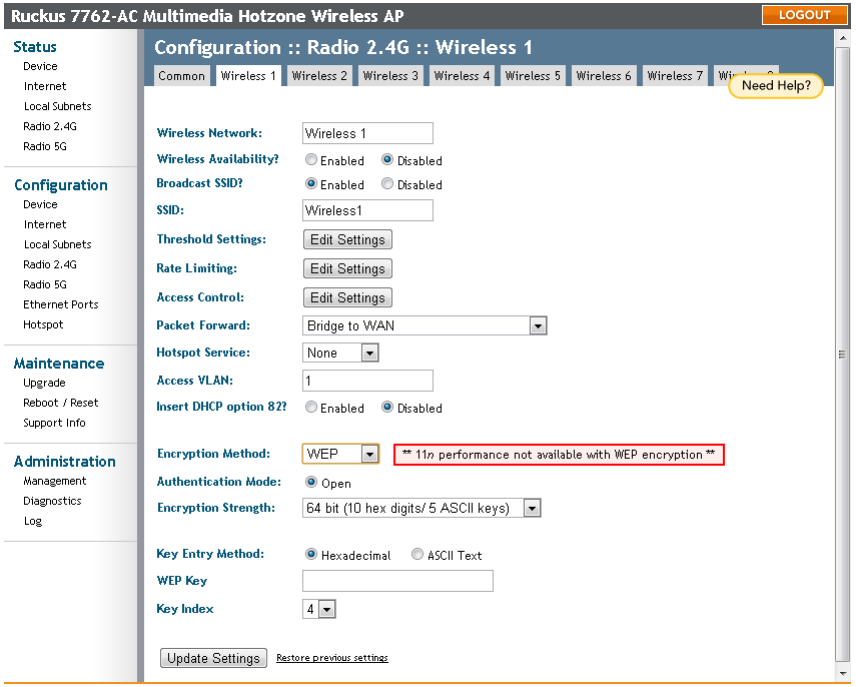
Using WEP

Wired Equivalent Privacy (WEP) is a security algorithm for 802.11 wireless networks designed to provide data confidentiality comparable to that of a wired network. WEP uses a pre-shared key for encrypting data frames that is shared among all users of the wireless network. For this reason and others, WEP has been discredited as a security mechanism and should be avoided in favor of WPA if at all possible.

CAUTION: WEP encryption has been proven to be easily circumvented. Therefore, Ruckus Wireless recommends using WPA whenever possible, and only use WEP if your client devices do not support WPA.

CAUTION: Using WEP encryption limits the performance of the AP to 802.11g rates. If you select WEP encryption for a WLAN, wireless devices that are capable of faster 802.11n transfer rates will be limited to 802.11g rates.

Figure 26. WEP settings



To configure WLAN-specific WEP encryption settings

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the **Wireless #** tab that you want to configure. The Configuration > Wireless > Wireless[#] page appears.
3. Click the **Encryption Method** menu, and then click **WEP**. An additional set of WEP-specific encryption options appear on this page.
4. Review the encryption settings listed in Table 16, and then make changes as required.

Table 16. WEP Options

Encryption Setting	Description
Authentication Mode	Open is the only authentication mode available with WEP encryption.
Encryption Strength	• 64 bit: Specify the key with 10 hexadecimal digits or 5 ASCII characters. • 128 bit: Specify the key with 26 hexadecimal digits or 13 ASCII characters. The 128-bit cryptography is stronger privacy protection for your network and is recommended if you use WEP.
Key Entry Method	• Hexadecimal: The encryption key only accepts hexadecimal characters (0-9, A-F). • ASCII Text: The encryption key accepts ASCII characters.
WEP Key	Enter the key manually according to the Key Entry Method and Encryption Strength settings.
Key Index	Choose the index, from "1" to "4", that the WEP key is to be stored in.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.
6. Click **Go back to Wireless Configuration** to reopen the previous page.

Using WPA

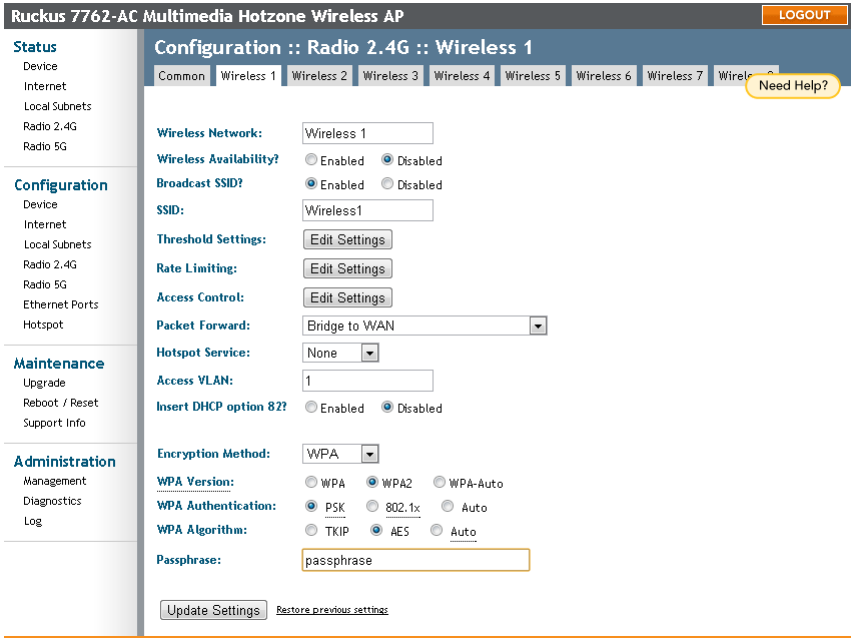
Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols developed by the Wi-Fi Alliance in response to the weaknesses of WEP.

Selecting WPA as the Encryption Method allows you to choose WPA version, WPA Authentication and WPA Algorithm. This section discusses WPA-PSK (pre-shared key). For information on WPA-Enterprise (WPA-802.1X), see "Customizing 802.1X Settings" on page 58.

Use of WPA-PSK (also known as WPA-Personal) allows automatic key generation based on a single passphrase. WPA-PSK provides strong security for home and small offices and does not require a RADIUS server, but may not be supported on older wireless devices. In some cases, the older devices can be upgraded with adapters to take advantage of WPA-PSK.

If you configure the WLAN with WPA-PSK, wireless users will not be able to connect to your WLAN unless their devices support WPA-PSK and are configured with the same passphrase.

Figure 27. WPA settings



To configure WPA encryption settings

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the Wireless # tab that you want to configure. The Configuration > Wireless > Wireless[#] page appears.
3. Click the **Encryption Method** menu, and then click **WPA**. An additional set of WPA-specific options appear on this page.
4. Review the encryption settings listed in Table 17, and then make changes as preferred.

Table 17. Encryption settings

Encryption Setting	Description
WPA Version	Your options are WPA, WPA2 or WPA Auto. • **WPA** (Wi-Fi Protected Access) is the replacement security standard adopted by the Wi-Fi Alliance in response to the security weaknesses of WEP. WPA was developed as an interim measure prior to the ratification of the 802.11i standard, which introduced WPA2. • **WPA2** provides stronger wireless security than WPA and is the recommended option. However, older wireless clients may not be compatible with WPA2. For example, WPA2 support on Windows XP requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later. • **WPA-Auto** allows both WPA and WPA2 devices to operate on the same WLAN.
WPA Authentication	**PSK** (Pre-Shared Key) mode is suitable for home or personal use. **802.1X** mode uses a RADIUS server to verify user identity. The auto mode offers both options for the wireless client to choose from. For more information on how to configure the 802.1X mode, refer to "Customizing 802.1X Settings" on page 58.

WPA Algorithm	• **TKIP**: Temporal Key Integrity Protocol is an older encryption algorithm that provides stronger security than a shared WEP key, but not as strong as the newer AES algorithm. • **AES**: AES (Advanced Encryption Standard) replaces TKIP as the default (and recommended) encryption algorithm for modern wireless LANs. • **Auto**: Auto allows both encryption algorithms to be used on the same WLAN. When Auto is selected, the wireless client decides whether TKIP or AES will be used. Note however that allowing TKIP will reduce the performance of the WLAN (as broadcast packets will be limited to slower transfer rates), and is therefore not recommended.
Passphrase	Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.
6. Click **Go back to Wireless Configuration** to reopen the previous page.

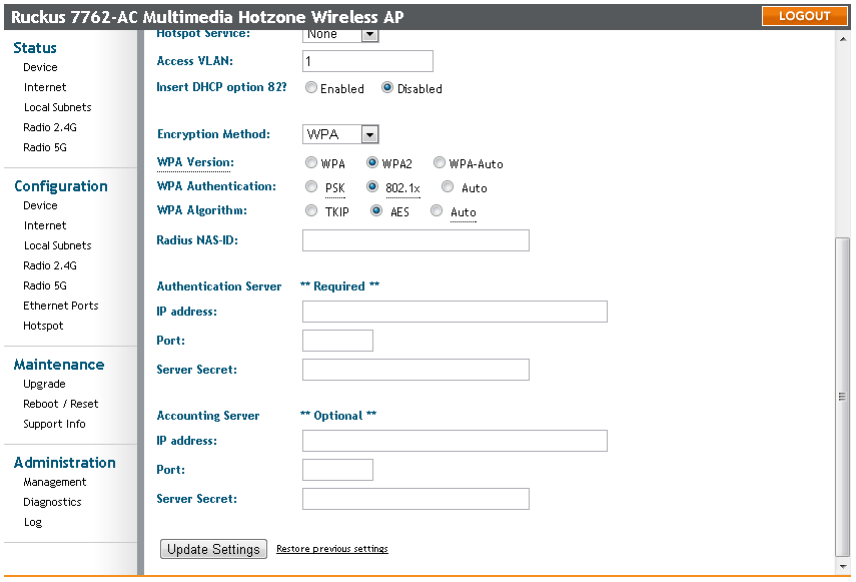
Customizing 802.1X Settings

CAUTION: Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

If you choose WPA as the encryption method, you have the option to set up the Access Point to act as an 802.1X proxy, utilizing external authentication sources such as a RADIUS server.

In 802.1X authentication, the supplicant sends access request messages along with credentials, such as user name / password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification. The supplicant (client device) remains in an unauthorized state until verification has been received. In unauthorized state, only 802.1X traffic is allowed; all other traffic, such as DHCP and HTTP traffic, is dropped. For its wireless interfaces, the Access Point can serve as the authenticator communicating between the supplicant and the authentication server.

Figure 28. 802.1X settings



To configure 802.1X authentication settings on a WLAN

1. Go to **Configuration** > **Wireless**. The Configuration > Wireless > Common page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click a **Wireless #** tab to configure. The Configuration > Wireless > Wireless[#] page appears.
3. Click the **Encryption Method** menu, then click **WPA**. The basic set of WPA-specific encryption options appears on the page.
4. Select **802.1X** as the WPA Authentication mode. Additional options appear.
5. Configure the following settings to customize your 802.1X authentication:
   - **RADIUS NAS-ID**: Enter the network ID assigned to your RADIUS server.
   - **Authentication Server [-Required-]**: Enter the information needed to establish a connection between the Access Point and the RADIUS server.
   - **Accounting Server [-Optional-]**: Enter the information needed to establish this connection.
6. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.
7. Click **Go back to Wireless Configuration** to reopen the previous page.

Setting Threshold Options

The following options allow you to fine-tune the "Protection Mode" behavior, set previously on the *Configuration > Wireless > Advanced > Common* page. After activating a Protection Mode, you can open each Wireless tab and customize the threshold settings, which determine what is put into effect and when.

CAUTION: Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

To customize Protection Mode (Threshold) settings

1. Go to **Configuration > Wireless**. The *Configuration > Wireless > Common* page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the tab for the Wireless # (WLAN) that you want to configure. The *Configuration > Wireless > Wireless [#]* page appears.
3. Look for **Threshold Settings**, and then click **Edit Settings**. The *Configuration > Wireless > Advanced > Wireless [#]* page appears.
4. Review the options listed in Table 18, and then make any needed changes.

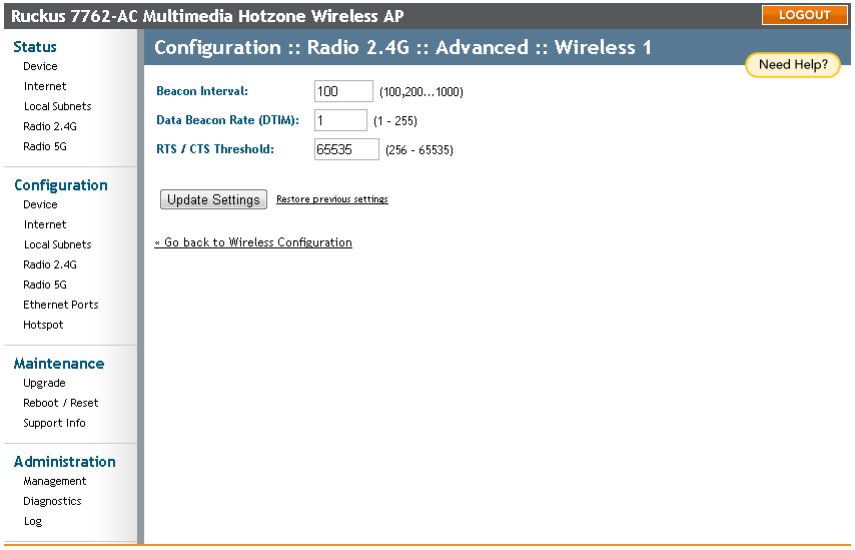
Table 18. Threshold options

Option	Description
Beacon Interval	(The default value is 100.) The value indicates the frequency interval of the beacon in milliseconds. A beacon is a broadcast packet sent by the AP to synchronize the wireless network.
Data Beacon Rate (DTIM)	(The default value is 1.) The value indicates the interval of the Delivery Traffic Indication Message (DTIM). This is a countdown field that the device uses to inform its clients of the next window for listening to broadcast or multicast messages.
RTS/CTS Threshold	(The default value is 65535.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in an environment with excessive signal noise or hidden nodes, but may result in some performance degradation.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

You have completed configuring the threshold options. To reopen the previous page, click the **Go back to Wireless Configuration** link.

Figure 29. Threshold settings



Rate Limiting

Rate Limiting allows you to cap the per client data transfer rates for a specific WLAN.

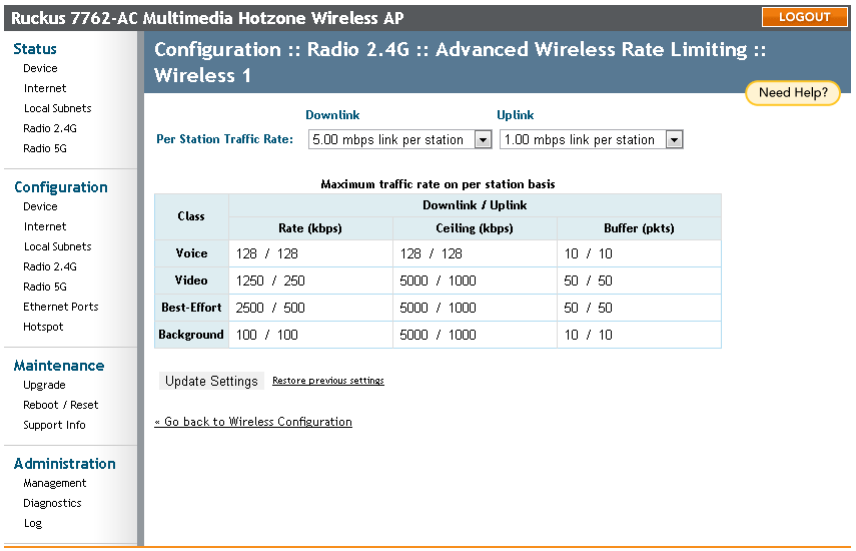
To enable per station rate limits

1. Go to **Configuration > Wireless**.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Select the WLAN that you want to configure from the tabs at the top of the page.
3. Click the **Edit Settings** button next to *Rate Limiting*. The *Rate Limiting* page appears.
4. Set the maximum **Downlink** and **Uplink** rate per station.
5. The table below updates to show the maximum transfer rate per station for each traffic type.
6. Click **Update Settings** to save your changes.

Figure 30. Limit per station traffic rates on a specific WLAN



Controlling Access to the Wireless Network

Access Control enables you to specify the stations are allowed to join (associate with) your wireless networks. Access controls can be configured for each WLAN from its respective *Wireless #* tab.

Access Control Options

This section describes the options that you can use to control access to the wireless network.

- **Disabling WLAN Access Restrictions**: If you select **Disable WLAN access restrictions**, then MAC-address-based restrictions on which stations can join the WLAN are disabled; thus, any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption passphrase. The Access Controls table is hidden if the current mode is **Disable WLAN access restrictions**.
- **Allowing Only Stations Listed in the Access Control Table**: If you select **Allow only stations listed in the Access Control Table**, then stations entered into the access-controls table are allowed but all others are disallowed. To add MAC addresses, see "Changing the Access Controls for a WLAN" on page 63.
- **Denying Only Stations Listed in the Access Control Table**: If you select **Deny only stations listed in the Access Control Table**, then stations entered into the access-controls table are disallowed but all others are allowed. To add MAC addresses, see "Changing the Access Controls for a WLAN" on page 63.

Changing the Access Controls for a WLAN

By default, the **Disable WLAN access restrictions** option is selected, which allows any wireless station to gain access to the wireless network. If you want to change this setting, follow the instructions below.

Figure 31. Access control settings

To edit the ACL

1. Go to **Configuration** > **Wireless**.

NOTE: If you are using a dual band ZoneFlex AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the **Wireless #** tab for which you want to configure the access control settings.
3. Click the **Edit Settings** button next to *Access Control*.
4. Select the radio button for the desired access control. (For a description of the options, see "Access Control Options" in the previous section.) The Access Controls Table appears.
5. To add a MAC address to the Access Control table, click the **Add new entry** button.
6. Fill out the following text boxes:
   - **Address**: Six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. You can specify a full 12-hex-digit MAC address or enter "wildcard" characters for "don't care" digits. Allowable hex-digit characters are 0-9, a-f, and A-F. Most address-tags and software where you find MAC addresses listed include colons or dashes to separate the address-pairs; that is provided for you on the web page, so do not enter the colons or dashes.

     Supported wildcard characters include "x", "X" and blank (space character). Wildcards are useful when you want to specify all MAC addresses from a given manufacturer. For example, by specifying only the Organizationally Unique Identifier (the first six hexadecimal digits of any MAC address from that manufacturer is its OUI) saves you having to enter all 24 million of them (the table size is limited in the AP/Router to 128 entries). Some manufacturers produce devices using more than one OUI, in which case you may need to enter each applicable one.
7. Click **Update** to save your changes. Assuming all parameters you entered are acceptable, that row will be added to the table.

You have completed adding an entry to the MAC address table. If you have additional MAC addresses you want included, click **Add new entry**, and then repeat these steps until you have entered all the stations you want. There is a limit of 128 rows.

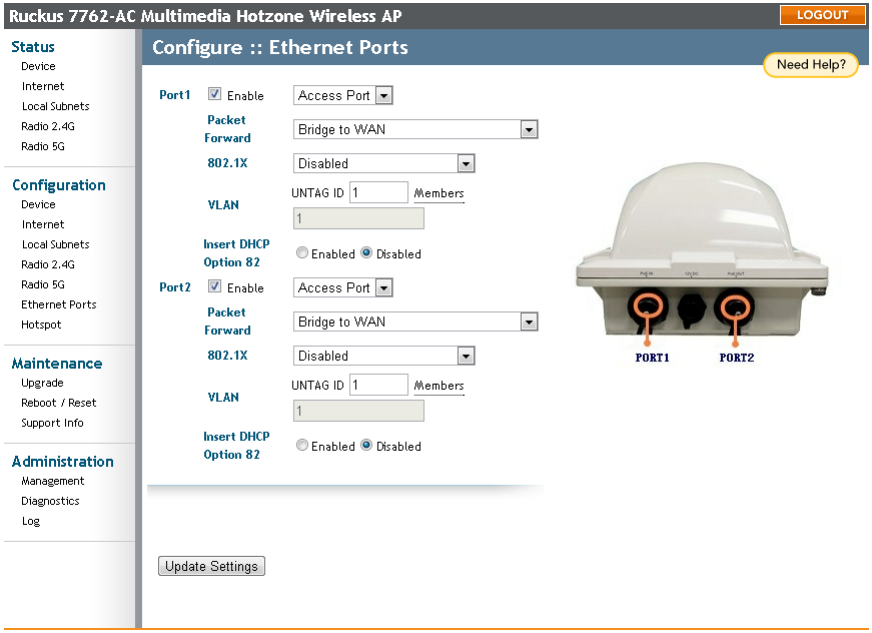
Removing a MAC Address

To remove a MAC address from the ACL table, click the **Cancel** button under the *Remove* column, and then click **Update**. The ACL table refreshes, and the MAC address that you deleted disappears from the table.

Configuring Ethernet Ports

The Ethernet Ports configuration page allows you to define how the Access Point's Ethernet ports behave. You can disable ports entirely, define trunking and packet forwarding behavior, configure 802.1X authentication settings, and configure VLAN settings for each port individually from this page.

Figure 32. The Configuration > Ethernet Ports page



To configure LAN ports

1. Go to **Configuration > Ethernet Ports**.
2. Review the following table and make changes as needed for each of the ports labeled **PORT 1** through **PORT 4** (depending on AP model), which correspond to the AP's Ethernet ports.

Setting	Description
Enable	All Ethernet ports are enabled by default. Unchecking this box next to a port disables that port entirely. If you do not want to provide wired access through the AP, uncheck (clear) the **Enable** box next to each LAN port.

Port Type	See "Setting Ethernet Port Type" on page 67 for more detailed information. ■ **Trunk Port**: This port passes all VLAN traffic. ■ **Access Port**: This port provides network access. ■ **General Port**: User-defined VLAN membership.
Packet Forward	**Isolated**: Selecting Isolated causes the traffic from this port to terminate at the Access Point. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this port to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
Local Subnet	This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forward*, and you have selected *Access Port* as the port type. This option allows you to select which subnet this port's traffic will be part of. You must have previously configured a subnet from the *Configuration > Local Subnets* page before it becomes available here.
802.1X	Configure the port as an 802.1X authenticator or supplicant. The following options are available: ■ **Disabled**: No 802.1X controls are applied to this port. ■ **Authenticator (Port Based)**: Only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. ■ **Authenticator (MAC Based)**: Each MAC host is individually authenticated. ■ **Supplicant**: The port acts as a supplicant to an upstream authenticator. Configure a port as Supplicant if the port is a Trunk Port used to connect the AP to a LAN switch. See "Working with 802.1X on Wired Ethernet Ports" on page 68 for more information.
VLAN	**Untag ID**: Enter a valid VLAN ID in this field to segment traffic arriving on this port to a specific VLAN. Default is 1. Valid VLAN entries are 1-4094. **Members**: Displays the VLAN membership of the port. (Membership is configurable only for the General port type.) See "Working with Port-Based VLANs" on page 69 for more information.

Insert DHCP Option 82	When this option is enabled for an Ethernet port, additional information will be encapsulated in DHCP option 82 and inserted into DHCP request packets. Current format of option 82 is: `Circuit ID sub-option: ETH:<IFNAME>:<VLAN>:N/A:<MODEL>:<HOSTNAME>:<DEVMAC>` This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

3. Click **Update Settings** to save your changes.

Setting Ethernet Port Type

ZoneFlex AP Ethernet ports can be configured as one of the following port types:

- Trunk Port
- Access Port
- General Port

Trunk Port

Trunk Ports forward and receive tagged and untagged frames and are used for bridging switch ports together. The Trunk port is a member of all VLANs that exist on the switch, and all VLAN-tagged traffic arriving on the port is seen. If an untagged frame is received on a Trunk port, the frame is associated with the Untag VLAN (also known as "native VLAN", by default, 1).

If a port is configured as a Trunk port, the Untag ID field can be used to define the Untag VLAN--the VLAN that the switch uses for forwarding/filtering purposes when a frame arrives without an 802.1Q header.

Access Port

Access Ports are used to provide network access. Traffic arriving on different Access Ports can be segmented into different logical networks (VLANs) using the Untag VLAN ID field. Access Ports are members of only one VLAN--the VLAN that is configured in the Untag VLAN field.

General Port

The General Port can be configured to support multiple tagged VLANs and one untagged VLAN. As Trunk Ports by definition are members of all VLANs, the General Port is the only port type for which membership is user configurable.

Working with 802.1X on Wired Ethernet Ports

802.1X authentication consists of the following three components:

- *Supplicant*: The supplicant sends access request messages along with credentials, such as user name / password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification.
- *Authenticator*: The authenticator challenges the identity of the supplicant, then passes its credentials to the AAA server. If the credentials are accepted the supplicant is allowed access.
- *Authentication Server (AAA Server)*: The AAA server verifies the supplicant's credentials and permits or rejects its request for access.

For wired 802.1X, a Ruckus AP's Ethernet port can be configured as either an *Authenticator* or as a *Supplicant*, depending on which port type is selected. Table 19 and Table 20 describe the 802.1X roles available by port type.

Table 19. Authenticator support by port type

	Trunk Port	Access Port	General Port
Port-based mode	X	X	X
MAC-based mode		X	

Table 20. Supplicant support by port type

	Trunk Port	Access Port	General Port
Supplicant	X		

The following considerations apply:

- A single port cannot be configured as both an *Authenticator* and *Supplicant* at the same time.
- Only one port per AP can be configured as a *Supplicant*.
- If the AP is connecting to a switch port with 802.1X authentication enabled, the AP's port type should be configured as a Trunk Port and its role should be configured as *Supplicant*. The switch port should be configured as a Trunk port in *Port-based Authenticator* mode.
- If there are multiple devices connected to an AP port (through a downstream switch), the port can be configured as either *Port-based* or *MAC-based Authenticator*. In Port-based mode, only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. In MAC-based mode, each MAC host is individually authenticated.
- If a Trunk Port is configured as a *Supplicant*, a user name and password must be entered to authenticate the port to the 802.1X aware LAN switch.

- If an Access Port is configured as an *Authenticator*, the administrator must define the RADIUS server that the Authenticator will communicate with. All Ethernet ports of a single AP are configured with the same RADIUS server.

Enable MAC authentication bypass: If MAC authentication bypass is enabled, the port first attempts to authenticate the attached device by MAC address, and if that fails, it will try to authenticate the device using 802.1X.

Working with Port-Based VLANs

The Access Point provides options for segmenting all incoming traffic (both wireless and wired Ethernet traffic) into specific VLANs. There are two ways to segment incoming traffic into VLANs:

- Each of the wireless interfaces (SSIDs) can be configured with a specific Access VLAN ID: (**Configuration > Wireless > Wireless [#] > Access VLAN**).
- Each of the LAN ports can be configured with an Untag VLAN ID (**Configuration > Ethernet Ports > VLAN > Untag ID**).

For Ethernet ports, the behavior of the Untag VLAN ID depends on the Port Type selected. If the port is configured as a Trunk port, it will include all VLANs (1-4094) in its membership. The VLAN Untag ID field (default = 1) can be used to redefine the "Native VLAN" for the port.

If the Ethernet port is configured as an Access Port, it can be configured with only one Untag VLAN ID and its membership includes only that one VLAN.

If the Ethernet port is configured as a General Port, it can be configured to include multiple VLANs in its membership and one Untag VLAN.

Configuring the Hotspot Service

The hotspot service can be deployed on standalone ZoneFlex APs through the Web interface. At a minimum, you must configure a login redirect URL and a RADIUS server to which users will be authenticated. Additional options and controls are provided on subsequent pages.

To enable the Hotspot service

1. Go to **Configuration > Hotspot**.
2. Click **Enabled** next to *Hotspot Service*.
3. Review the settings in table Table 21, and make changes as needed.

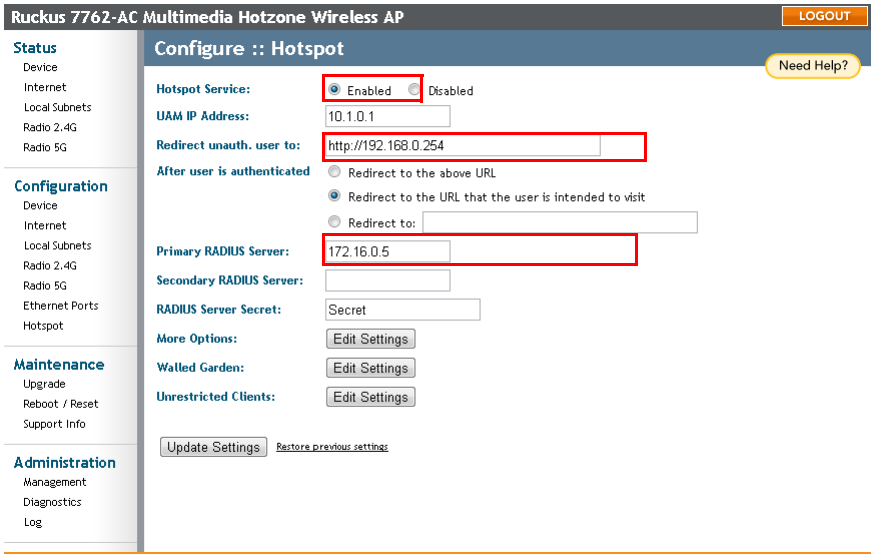
Table 21. Hotspot configuration settings

Setting	Description
UAM IP Address	Specify the IP address of the UAM service.
Redirect unauth. user to	Redirect unauthenticated users to the specified URL (login page).
After user is authenticated	Select where you want to redirect the user after successful authentication. • *Redirect to the above URL*: return to the login URL configured above. • *Redirect to the URL the user intended to visit*: upon successful authentication, go directly to the URL that the user originally entered (typically the browser's home page). • *Redirect to*: specify a URL to which users are redirected after authentication. This can be used to redirect users to a "Login Successful" page, or a page that offers connection time information or a Logout button.
Primary RADIUS Server	Enter the IP address of the primary RADIUS server against which users will be authenticated (required).
Secondary RADIUS Server	Enter the IP address of the secondary RADIUS server, if one is available (optional).
RADIUS Server Secret	Enter the shared secret for communication with the RADIUS server (required).

4. Click **Update Settings** to save your changes.

You have completed the minimum settings for providing Hotspot service on this AP. Additional configuration options are available using the *Edit Settings* buttons at the bottom of the page.

Figure 33. Minimum configuration settings for providing Hotspot service



Customizing Optional Hotspot Settings

Optional Hotspot settings include a number of options for fine-tuning your Hotspot service, such as maximum session time, grace period, and accounting update interval.

The following Hotspot options can be configured from the *Configuration* > *Hotspot* > *More Options* page:

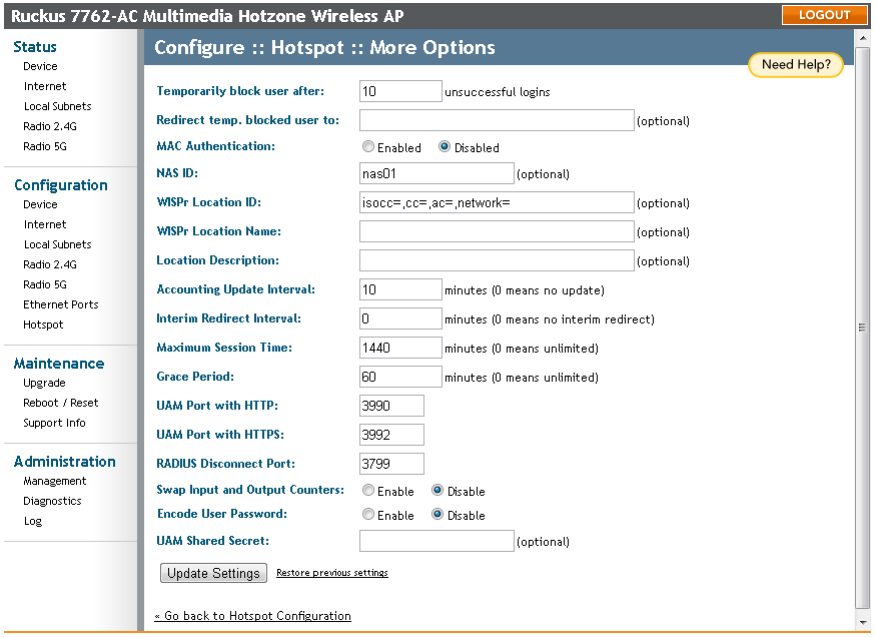
Table 22. Optional Hotspot settings

Setting	Description
Temporarily block user after __ unsuccessful login attempts	Specify the maximum number of repeated authentication failures allowed. Default = 10.
Redirect temp. blocked user to	Enter a redirect URL to which blocked users will be redirected. Default = (none).
MAC Authentication	If enabled, the Hotspot service will attempt to authenticate users based on their MAC addresses if the local Hotspot authentication has failed. If enabled, an optional MAC authentication password can be entered. If no password is specified, the system will use the client's MAC address as the password. Default = Disabled.

NAS ID	Specify the Network Access Server identifier of this device. The NAS-ID attribute is sent in RADIUS access and accounting request messages. It can also be used as location identification when NAS-IP-Address cannot be used for this purpose. Default = nas01.
WISPr Location ID	Specify the Hotspot location identifier, or WISPr (Wireless Internet Service Provider Roaming) location identifier. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of `"isocc=<ISO_Country_Code>, cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>"`. Default = `isocc=,cc=,ac=,network=`.
WISPr Location Name	Specify the hotspot location and operator's name. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of `"<HOTSPOT_OPERATOR_NAME>,<Location>"`. Default = (none).
Location Description	Specify the description of location. This value is provided in the HTTP redirection. Default = (none).
Accounting Update Interval	Specify the interval for RADIUS accounting requests. Default = 10 minutes.
Interim Redirect Interval	Specify the interval after which users will be redirected to the login URL. Default = 0 minutes.
Maximum Session Time	Enter the maximum session time in minutes. Default = 1440 minutes.
Grace Period	Specify the maximum time that a user may disconnect from the Hotspot service and return without the need to login again. Default = 60 minutes.
UAM Port with HTTP	TCP port to bind to for authenticating clients using HTTP. Default = 3990.
UAM Port with HTTPS	TCP port to bind to for authenticating clients using HTTPS. Default = 3992.
RADIUS Disconnect Port	UDP port to listen to for accepting RADIUS disconnect requests. Default = 3799.

Swap Input and Output Counters	Swap the value of input counters (packets, octets and giga words) and output counters in RADIUS accounting requests. This option is mainly for backward compatibility with existing Chillispot deployments. Default = Disable.
Encode User Password	Encode user password with challenge string, if UAM secret is not specified; otherwise, encode user password with both challenge string and UAM secret. Default = Disable.
UAM Shared Secret	The UAM Shared Secret is the shared secret between this Access Point and the HTTP server for the Redirection URL. Default = (none).

Figure 34. Configuring optional Hotspot options



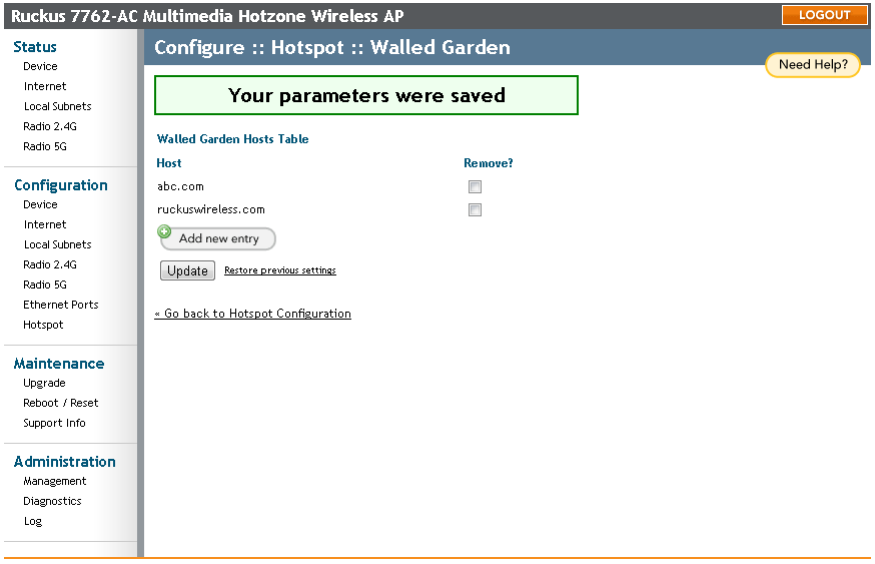
Creating a Hotspot Walled Garden

You can use the Hotspot Walled Garden rules to designate network destinations (host address or subnet) that users can access without going through authentication. A Walled Garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the Walled Garden. URLs will be resolved to an IP address (up to four). Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to reauthenticate when they navigate through the page.

To create Walled Garden rules

1. Go to **Configuration > Hotspot > Walled Garden**.
2. Click **Add new entry**. A field entitled *Walled Garden Hosts* appears.
3. In *Walled Garden Host*, enter a host name, IP address, network segment (e.g., 192.168.1.0/24) or a domain name. If a domain name is entered, it will be resolved every 5 minutes.
4. Click **Update** to save your entry.
5. You can create up to 64 entries in the Walled Garden Hosts table. Repeat the preceding steps as required.

Figure 35. The Walled Garden hosts table



To remove entries from the Walled Garden hosts table

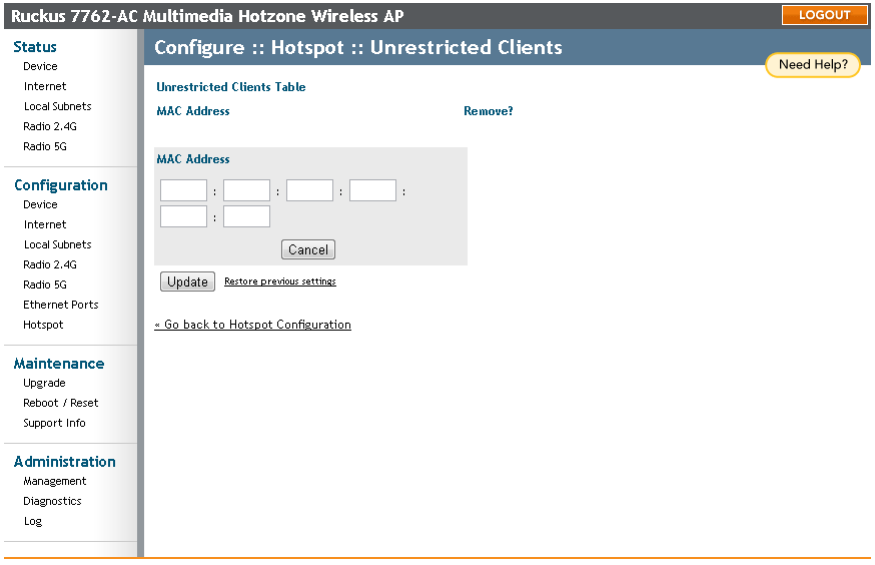
1. Click the check box next to the entry you want to remove, under the **Remove?** column.
2. Click **Update**. The entry is removed from the list.

Allowing Unrestricted Access by MAC Address

To allow selected clients unrestricted access to your Hotspot service:

1. Go to **Configuration > Hotspot > Unrestricted Clients**.
2. Click **Add new entry**.
3. Enter the MAC address of the client.
4. Click **Update** to save your changes.
5. Repeat the preceding steps as required.

Figure 36. Configuring Hotspot unrestricted clients table



5

Managing the Access Point

In This Chapter

Viewing Current Device Settings 78
Viewing Current Internet Connection Settings 79
Viewing Current Local Subnet Settings 80
Viewing Current Wireless Settings 81
Viewing Associated Wireless Clients 83
Changing the Administrative Login Settings 84
Enabling Other Management Access Options 85
Working with Event Logs and Syslog Servers 90
Upgrading the Firmware 93
Rebooting the Access Point 96
Resetting the Access Point to Factory Defaults 97
Running Diagnostics 98
Where to Find More Information 100

This chapter provides instructions for managing standalone ZoneFlex Access Points using the Web interface. For information on managing your ZoneFlex network using ZoneDirector, refer to the *ZoneDirector User Guide*, available from the Ruckus Wireless website.

Viewing Current Device Settings

The Status > Device page displays a general overview of the AP's current status, including AP name, serial number, MAC address, current software version, and so forth.

Figure 37. The Status > Device page

Viewing Current Internet Connection Settings

The Status > Internet page displays information on the AP's network settings; i.e., the settings that allow the AP to communicate with your local network and the Internet. Information includes IP address, gateway, DNS server, NTP server, and connection type (method of obtaining an IP address -- DHCP or static IP).

Figure 38. The Status > Internet page

Viewing Current Local Subnet Settings

The Status > Local Subnets page can be used to view the router (local subnet) configurations and list of any clients connected to those subnets.

If you want to make changes to any of these settings, go to **Configuration > Local Subnets**. Refer to "Configuring Local Subnets" on page 44 for more information.

Figure 39. The Status > Local Subnet page

Viewing Current Wireless Settings

If you want to view the current common wireless settings that the AP is using, go to the **Status** > **Wireless** page (on dual band APs, go to **Status > Radio 2.4G** or **Status > Radio 5G**). Table 23 lists the descriptions of each common wireless setting.

Table 23. Common Wireless settings

Setting	Description
Wireless Mode	Shows the wireless mode that the AP is currently using. Possible values include: • Auto-Select • 2.4GHz 54 Mbps • 2.4GHz 11 Mbps • 11ng (Operates with 802.11n, 802.11g and 802.11b devices in 2.4GHz spectrum only) • 11na (Operates with 802.11n and 802.11a devices in 5GHz spectrum only)
Channel	Shows the wireless channel that the AP is currently using. If you set the wireless channel to SmartSelect, this field will show the value **Channel # [SmartSelect]**.
Channel Width	11n devices only. Displays whether the channel width is set to 20MHz or 40MHz.
Country Code	Shows the country code that the AP has been set to use. *CAUTION: Verify that the AP is using the correct country code to make sure it uses only the allowed radio channels in your region. Selecting the incorrect country code may result in violation of application laws.*
AeroScout RFID tag detection	Shows **Enabled** if you enabled AeroScout RFID tag detection. The default setting is **Disabled**.
AeroScout Engine communication daemon	Shows **Up** if the communication agent on the AP is able to relay location data from AeroScout Tags to the AeroScout Engine. If the communication agent is unable to relay data or AeroScout tag detection is disabled, this field will show **Down**.

If you want to make changes to any of these settings, go to the **Configuration** > **Wireless** page. Refer to "Configuring Common Wireless Settings" on page 46 for more information.

Figure 40. The Status > Wireless (Radio 2.4G/5G) page

Viewing Associated Wireless Clients

A usage-monitoring capability has been built into the Access Point to help you monitor wireless clients that are associated with your wireless network.

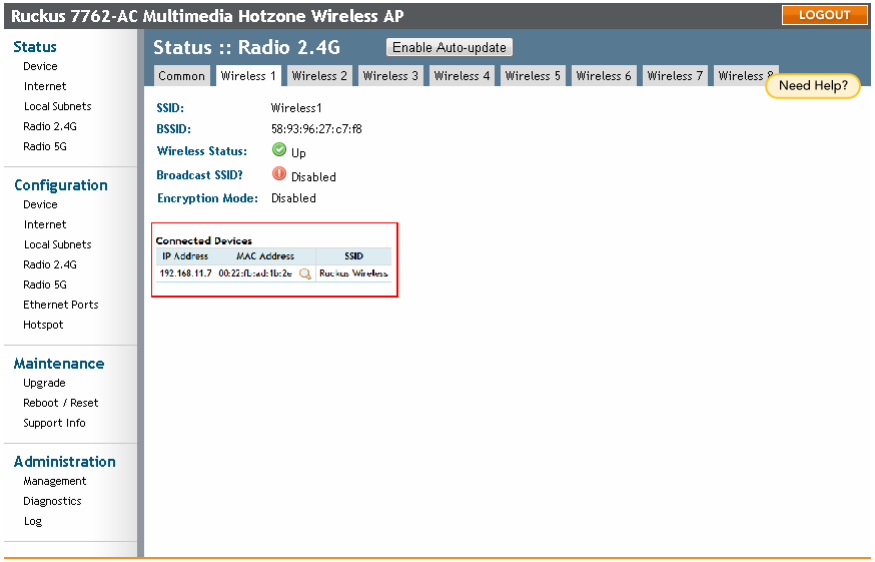
To view associated wireless clients

1. Go to **Status** > **Wireless**. The Status > Wireless page appears.

NOTE: If you are using a dual band ZoneFlex AP, go to **Status** > **Radio 2.4G** or **Status** > **Radio 5G.**

2. Click any of the **Wireless** tabs. Wireless clients that are associated with this particular wireless network appear under **Connected Devices**.

Figure 41. Viewing connected devices



Changing the Administrative Login Settings

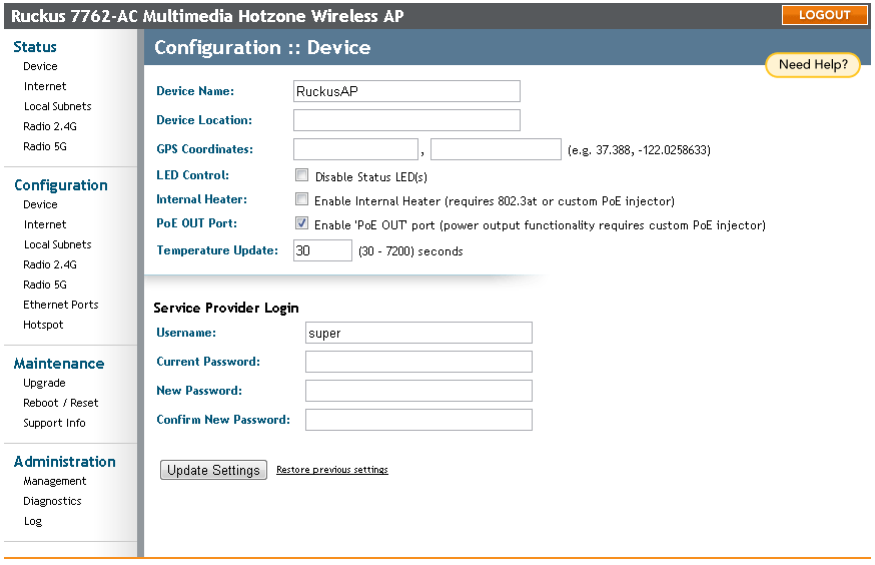
The default user name is `super` and the default password is `sp-admin`. To prevent unauthorized users from logging in to the Web interface using these default administrator login settings, Ruckus Wireless recommends that you change the default Web interface password immediately after your first login.

To change the default administrator login settings

1. Log in to the Web interface.
2. Go to **Configuration** > **Device**. The Device page appears.
3. Under **Service Provider Login**, change the default administrator login settings.
   - In **Username**, type a new user name that you will use to log in to the Web interface. The default user name is `super`.
   - In **Current Password**, type an existing password. The default password is `sp-admin`.
   - In **New Password**, type a new password to replace the existing password. The password must consist of six to 32 alphanumeric characters only.
   - In **Confirm New Password**, retype the new password.
4. Click **Update Settings**. The message *Your parameters were saved* appears.

You have completed changing the default login settings. The next time you log in to the Web interface, make sure you use these updated login settings.

Figure 42. The Configuration > Device page



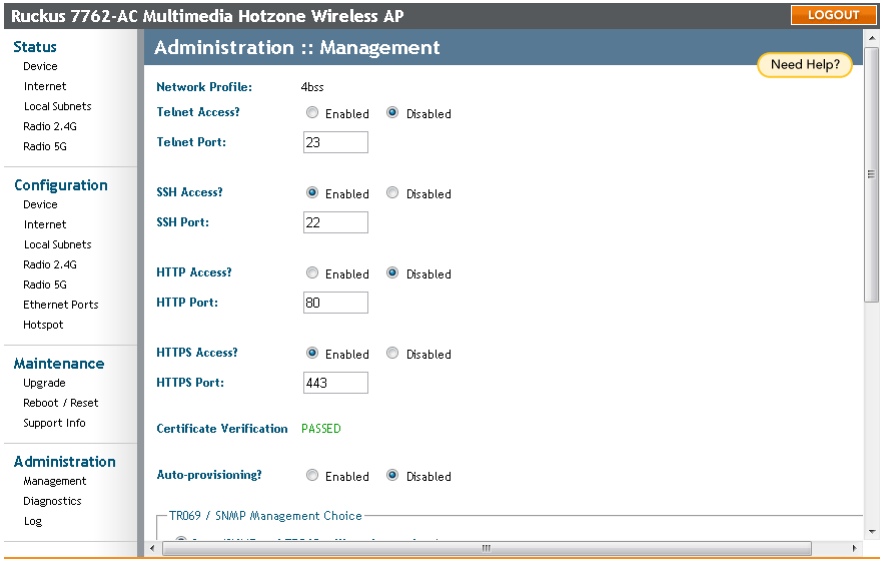
Enabling Other Management Access Options

In addition to managing the AP via a Web browser through HTTPS, several other management access options are available on the AP. These options include management access via HTTP, Telnet and SSH.

You can also view and set up the connection to a Ruckus Wireless FlexMaster server under the **TR-069/SNMP Management Choice** options. If your ZoneFlex AP is to be managed by FlexMaster, then the FlexMaster information (server URL and contact interval) is preconfigured before you receive your ZoneFlex AP.

NOTE: If you are configuring the AP to be managed by FlexMaster, remember to point it to the FlexMaster server after you configure the management access options. For more information, refer to "Viewing FlexMaster Management Status" on page 88.

Figure 43. The Administration > Management page



To enable other management access options

1. Go to **Administration** > **Management**. The Management page appears.
2. Review the access options listed in Table 24, and then make changes as needed.

Table 24. Management Access Options

Option	Description
Telnet Access	By default, this option is disabled (inactive).
Telnet Port	This field lists the default Telnet port of 23 — only if Telnet is active. You can manually change this port number, if required.
SSH Access	By default, this option is enabled (active).
SSH Port	This field lists the default SSH port of 22—only if SSH is active. You can manually change this port number if required.
HTTP Access	This option is disabled by default.
HTTP Port	This field lists the default HTTP port of 80, if HTTP has been activated. You can manually change this port number if required.
HTTPS Access	By default this option is enabled. This connection mode requires a security certificate, a copy of which has been pre-installed in the AP.
HTTPS Port	This field lists the default HTTPS port of 443—only if HTTPS has been activated. You can manually change this port number if required.
Certification Verification	This notes whether the security certificate linked to the HTTPS settings has been passed or not.
Auto-provisioning	This setting is disabled by default, and should only be enabled if using FlexMaster server for AP management.

3. If you want to use TR-069 or SNMP to manage the AP, configure the settings listed in Table 25.

Table 25. TR-069 and SNMP Management Options

Option	Description
Auto	Enables ZoneFlex AP management by SNMP server, Ruckus Wireless ZoneDirector or Ruckus Wireless FlexMaster
SNMP only	Only allow SNMP management
FlexMaster only	Only allow FlexMaster management
None	Disables ZoneFlex AP management by SNMP server, ZoneDirector and FlexMaster
DHCP Discovery	URL of server providing DHCP
FlexMaster Server URL	URL of the FlexMaster server
Digest-authentication Username/Digest-authentication Password	This information is automatically generated by the AP and used for authentication with FlexMaster. Change this value *only* if you want the AP to connect to another access control server (ACS).
Periodic FlexMaster Inform Interval	Interval at which the AP should attempt to contact FlexMaster

4. Click **Update Settings** to save your changes. A confirmation message appears at the top of the page.

You have completed configuring the management access options.

NOTE: Remember to open any relevant firewall ports between the AP and the firmware upgrade/management server. For example, if HTTPS is used for firmware upgrades, open TCP port 443 on the firewall to allow connections through port 443. If FlexMaster server is used, open TCP ports 80 and 443 for HTTP/HTTPS communications, and TCP port 8082 for AP wake-up commands.

Viewing FlexMaster Management Status

If you configure the AP to be managed by FlexMaster, you can check the *TR-069 Status* section on the **Administration** > **Management** page.

Figure 44. TR-069 status information

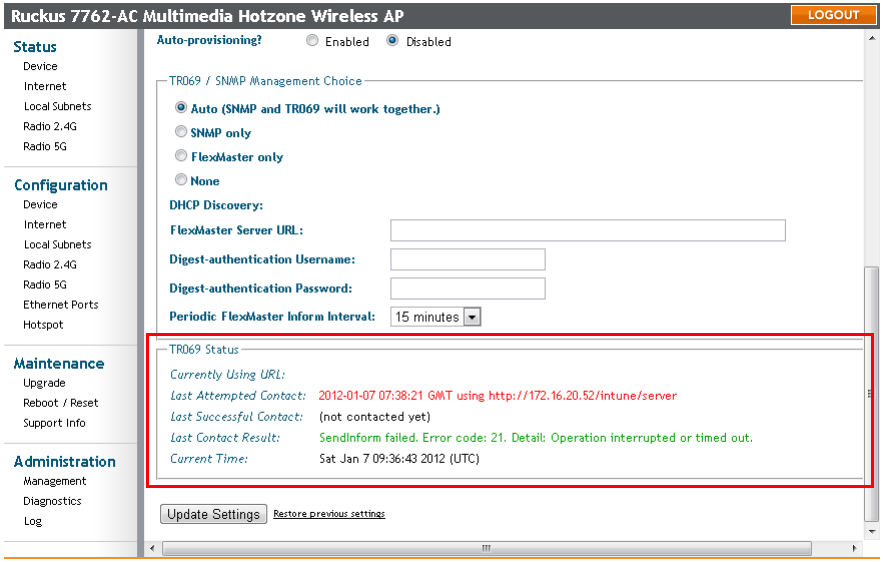


Table 26 lists the TR-069 status information that the AP provides.

Table 26. TR-069 status information

Status Information	Description
Currently using	Shows the FlexMaster server IP address or URL with which the AP is currently registered
Last Attempted Contact	Shows the date and time of the AP's last attempt to contact FlexMaster. Date and time are specified in GMT (or UTC), which are accurate if a Network Time Protocol (NTP) server is configured.
Last Successful Contact	Shows the date and time of the AP's last successful contact with FlexMaster.
Last Contact Result	Shows the result of the last attempt to contact FlexMaster (success or failure, and failure error code if applicable).
Current Time	Shows the current date and time as known to the AP. This timestamp is accurate if an NTP server is configured on the AP. If there is no NTP server configured, this timestamp is useful as a reference for comparison of the timestamps for **Last attempted contact** and **Last successful contact**.

Pointing the AP to FlexMaster

Your ZoneFlex AP is required to "call home" to register with your FlexMaster; FlexMaster does not initiate initial contact. To register successfully with FlexMaster, your ZoneFlex AP must know the FlexMaster server's URL, thus entered on the AP. You will need TCP ports 80 and 443 between APs and FlexMaster when traversing Layer 3/firewall boundaries.

To point the AP to FlexMaster

1. Go to **Administration > Management**.
2. Under **TR-069/SNMP Management Choice**, click **Auto**.
3. In **FlexMaster Server URL**, type the URL of the FlexMaster server.
4. Toggle the **Contact FlexMaster every** drop-down list to select how frequently the AP will check the FlexMaster server for any pending configuration changes available for that ZoneFlex unit. On the FlexMaster side, this field is referred to as the Periodic Inform Interval.
5. Click **Update Settings** to save your changes.

After the AP registers with FlexMaster, this **Administration > Management** page will show the communication status between the AP and FlexMaster.

Working with Event Logs and Syslog Servers

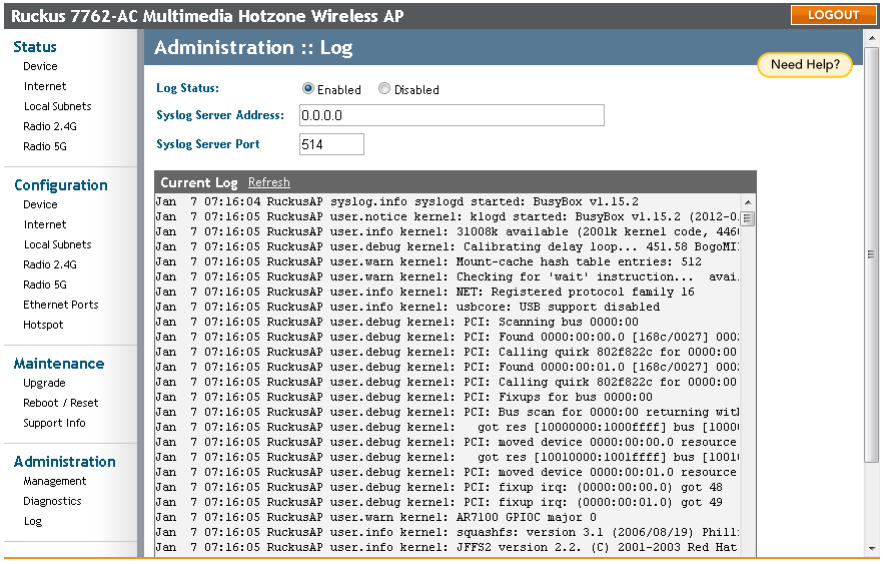
Both the *Maintenance* > *Support Info* and *Administration* > *Log* pages can be used to view the AP's current log file text. You can use the former to send the log to Ruckus Wireless support directly or save it to a local file, and use the latter to configure automatic delivery of log files to a syslog server.

Enabling Logging and Sending AP Events to a Syslog Server

If you have a syslog server on the network, you can configure the Access Point to send the AP logs to the server. You will need to enable logging (if disabled) and configure the Access Point to send its events to the syslog server.

1. Go to **Administration** > **Log**. The Administration > Log page appears.
2. Look for **Log Status,** and then click **Enabled**.
3. After enabling logging, configure the following options:
   - **Syslog Server Address**: To enable the AP to send messages to a syslog server as they appear, enter the IP address of the syslog server.
   - **Syslog Server Port**: By default, the syslog port number is 514. If the syslog server is using a different port, enter that port number in this field.
4. Click **Update Settings** to save and apply your changes.

Figure 45. The Administration > Log page


Ruckus 7762-AC Multimedia Hotzone Wireless AP
LOGOUT
Status
Device
Internet
Local Subnets
Radio 2.4G
Radio 5G
Configuration
Device
Internet
Local Subnets
Radio 2.4G
Radio 5G
Ethernet Ports
Hotspot
Maintenance
Upgrade
Reboot / Reset
Support Info
Administration
Management
Diagnostics
Log
Administration :: Log
Need Help?
Log Status:
Enabled
Disabled
Syslog Server Address:
0.0.0.0
Syslog Server Port
514
Current Log
Refresh
Jan 7 07:16:04 RuckusAP syslog.info syslogd started: BusyBox v1.15.2
Jan 7 07:16:05 RuckusAP user.notice kernel: klogd started: BusyBox v1.15.2 (2012-0
Jan 7 07:16:05 RuckusAP user.info kernel: 31008k available (2001k kernel code, 446
Jan 7 07:16:05 RuckusAP user.debug kernel: Calibrating delay loop... 451.58 BogoMI
Jan 7 07:16:05 RuckusAP user.warn kernel: Mount-cache hash table entries: 512
Jan 7 07:16:05 RuckusAP user.warn kernel: Checking for 'wait' instruction... avai
Jan 7 07:16:05 RuckusAP user.info kernel: NET: Registered protocol family 16
Jan 7 07:16:05 RuckusAP user.info kernel: usbcore: USB support disabled
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Scanning bus 0000:00
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Found 0000:00:00.0 [168c/0027] 000
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Calling quirk 802f822c for 0000:00
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Found 0000:00:01.0 [168c/0027] 000
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Calling quirk 802f822c for 0000:00
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Fixups for bus 0000:00
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: Bus scan for 0000:00 returning wit
Jan 7 07:16:05 RuckusAP user.debug kernel: got res [10000000:1000ffff] bus [1000
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: moved device 0000:00:00.0 resource
Jan 7 07:16:05 RuckusAP user.debug kernel: got res [10010000:1001ffff] bus [1001
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: moved device 0000:00:01.0 resource
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: fixup irq: (0000:00:00.0) got 48
Jan 7 07:16:05 RuckusAP user.debug kernel: PCI: fixup irq: (0000:00:01.0) got 49
Jan 7 07:16:05 RuckusAP user.warn kernel: AR7100 GPIOC major 0
Jan 7 07:16:05 RuckusAP user.info kernel: squashfs: version 3.1 (2006/08/19) Phill
Jan 7 07:16:05 RuckusAP user.info kernel: JFFS2 version 2.2. (C) 2001-2003 Red Hat

Sending a Copy of the AP Log File to Ruckus Wireless Support

You can set up a connection to an FTP or TFTP site to send a copy of the current AP log file to Ruckus Wireless Support. You can alternatively send the AP log file(s) as described in "Saving Copies of the Current AP Log Files to Your Computer" on page 91.

To send a copy of the current log file using FTP or TFTP:

1. Go to **Maintenance** > **Support Info**. The Maintenance > Support Info page appears.
2. In **Transfer Method**, click the TFTP or FTP option. Clicking the FTP option prompts you to enter a User ID and Password.
3. In **Server Address**, enter the FTP or TFTP server IP address.
4. In **Filename**, enter a name for this file that you are saving.

NOTE: Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host."

5. If required, in **Username** and **Password** enter a the login for the server.
6. Click **Upload Now**.

Saving Copies of the Current AP Log Files to Your Computer

You can send copies of the current AP log files to Ruckus Wireless Support by saving one or both files to your local PC, and then attaching them to an email message and sending them to support

- The Support info log (*supportinfo.txt*) includes the configuration and run-time status of the AP when it is managed by ZoneDirector.
- The Access Point log (*tr069info.txt*) includes the configuration and run-time status of the AP when it is in standalone mode and/or managed by FlexMaster.

To save a copy of the current AP logs to your own computer:

1. Go to **Maintenance** > **Support Info**. The Maintenance > Support Info workspace appears.
2. In **Transfer Method**, click **Save to Local Computer**. Two links appear next to **Download** (*supportinfo.txt* and *tr069info.txt*).
3. Click the **supportinfo.txt** link. A new window (or tab) opens with the contents of the log file displayed.
4. Choose **Save As** or **Save Page As** from your browser's **File** menu.

5. When the "Save as..." dialog box appears, find a convenient location on your local computer to save the file, and change the file extension from *html* to *txt*.
6. Click **Save** to save the *supportinfo.txt* file to your computer.
7. If required, repeat this procedure for the *tr069info.txt* file.

You have saved the AP log file(s) to your computer. You can now sent them to Ruckus Wireless Support.

Upgrading the Firmware

You can use the Web interface to check for software updates/upgrades for the firmware built into the AP. You can then apply these updates to the AP in one of two ways: (1) manual updating on an as-needed basis or (2) automating a regularly scheduled update.

Before starting, decide which option you want to take:

- Automate a regularly scheduled update
- Run a one-time manual update right now

By default, the automatic upgrade option is disabled.

To get started with upgrading the firmware, go to **Maintenance** > **Upgrade**. When the **Maintenance** > **Upgrade** options appear, decide which upgrade method to use. Each of the upgrade options listed on the Upgrade page are discussed in the succeeding sections.

Figure 46. The Maintenance > Upgrade page

Upgrading Manually via FTP or TFTP

1. In the **Upgrade Method** options, click **FTP** or **TFTP**.
2. Click the host name field, and then type the URL of the server. Or click the IP address field, and then type the IP address of the server. Remember to start the URL with `ftp://`.

CAUTION: Do not change any of the Image Control File, Username, or Password entries.

3. Click **Perform Upgrade**. A status bar appears during the upgrade process.
4. After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via the Web

1. In the **Upgrade Method** options, click **Web**.
2. If instructed to choose a different URL than the default value, click the **Web Options URL** field, and then type the URL of the download Web site. Remember to start the URL with "http://".
3. Click **Perform Upgrade**. A status bar appears during the upgrade process.
4. After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via Local File

If you have already saved a firmware file on your local computer, you can upgrade directly using the Web interface.

1. In the **Upgrade Method** options, choose **Local**.
2. Click the **Choose File** button and locate the file on your local computer.
3. Select the file and click **OK**.
4. Click **Perform Upgrade**. A status bar appears during the upgrade process.
5. After the upgrade is completed, you must manually reboot the AP.

Scheduling Automatic Upgrades

When the upgrade method is TFTP, FTP or Web, you can schedule automatic upgrades:

1. In the Upgrade Method options, click the button for your preferred choice.
2. Enter the appropriate information in the Host name field or IP address field.

CAUTION: Do not change any of the Image Control File, Username, or Password entries.

3. Verify that the Auto Upgrade option is set to **Enabled**.
4. Toggle the **Interval to Check for Software Upgrade** drop-down list to select your preferred interval.
5. Choose whether to reboot immediately after upgrading, or schedule the reboot for a specific time of day using the **Schedule Reboot Time After Upgrade** list. Choosing **Any Time** (the default value) results in the AP performing a reboot immediately after the automatic upgrade is successful.
6. You have two options at this point:
   - Click **Perform Upgrade**, which will start the process and the clock. The next upgrade will occur at the selected interval.
   - Click **Save parameters only**. The clock starts right away, and the actual upgrade will occur at the first effective interval.

   After you click one of these two options, a status bar appears during the upgrade process.

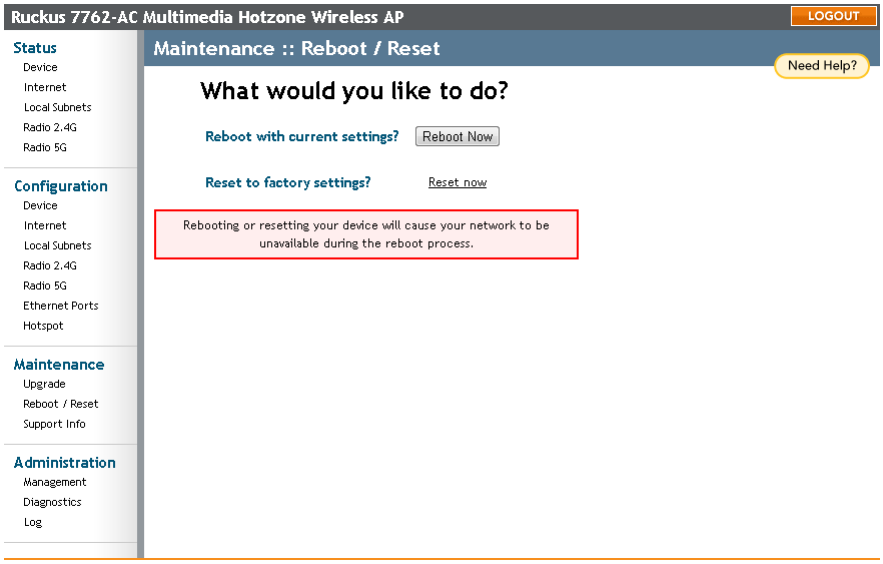
When the upgrade is complete, the AP will reboot automatically at the time you specified in step 5.

Rebooting the Access Point

You can use the Web interface to prompt the AP to reboot, which simply restarts the AP without changing any of the current settings. Please note that rebooting the AP will disrupt network communications in any currently active WLANs.

1. Go to **Maintenance** > **Reboot/Reset**. The Maintenance > Reboot/Reset page appears.
2. Click **Reboot Now**. After a brief pause, you will be automatically logged out of the AP.

Figure 47. The Maintenance > Reboot/Reset page



After approximately one minute, you should be able to log back into the AP, which verifies that the reboot was successful. You can also check the LEDs to verify the status of the AP.

NOTE: The 7761-CM Access Point can also be remotely reset using the OID and CLI commands described in the *ZoneFlex 7761CM Dual Band 802.11n Outdoor Access Point with Integrated Cable Modem Installation Guide*.

Resetting the Access Point to Factory Defaults

WARNING: DO NOT reset the Access Point to factory defaults unless you are directed to do so by Ruckus Wireless support staff or by a network administrator. Do this only if you are able to immediately connect the restored AP to your computer, to reconfigure it for Wi-Fi network use.

You can use the Web User interface to restore an inoperative AP to its factory default settings, which will completely erase the configuration currently active in the AP. Note, too, that this will disrupt all wireless network communications through this AP.

To reset the Access Point to factory defaults

1. Go to **Maintenance** > **Reboot/Reset**. The Maintenance > Reboot/Reset page appears.
2. Click **Reset now** (next to *Restore to factory settings*?).
3. When the confirmation warning appears, read the message and click **OK** if you are certain that you want to restore the AP to factory defaults.

After a brief pause, you will be automatically logged out of the AP. You must now disconnect the AP from the switch (and the network) and reconnect it to your computer, as described in the associated AP *Installation Guide*. At this time, you can restore the network settings, then replace it in your site for full network use.

Running Diagnostics

Two network connection diagnostic tools – ping and traceroute – have been built into the AP to help you check network connections from the Web interface.

To run diagnostics for network troubleshooting

1. Go to **Administrator** > **Diagnostics**. The Administrator > Diagnostics page appears. Two options are available:
   - Ping
   - Traceroute
2. Click the text field by the option you want to activate, and type the network address of a site you wish to connect to.
3. Click **Run test**.

The results appear in the text field below each option.

Figure 48. Pinging a client

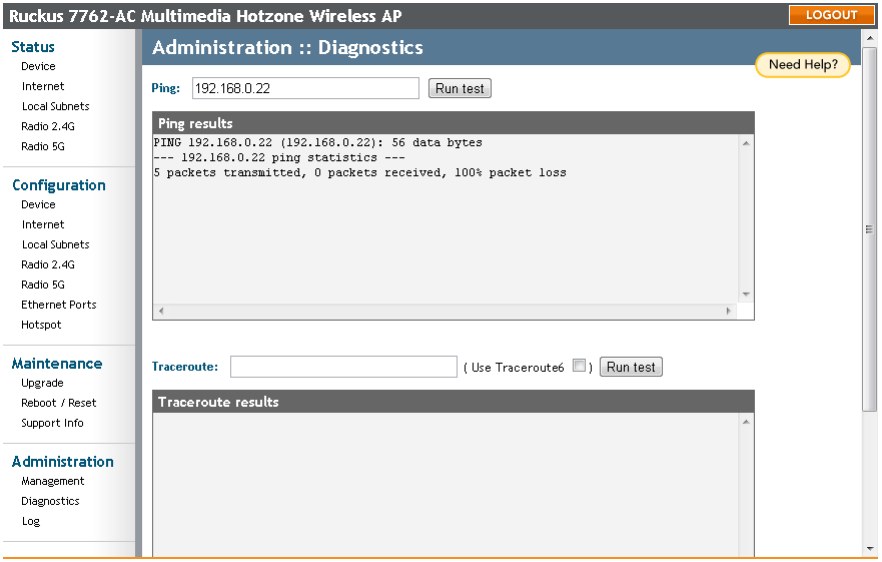
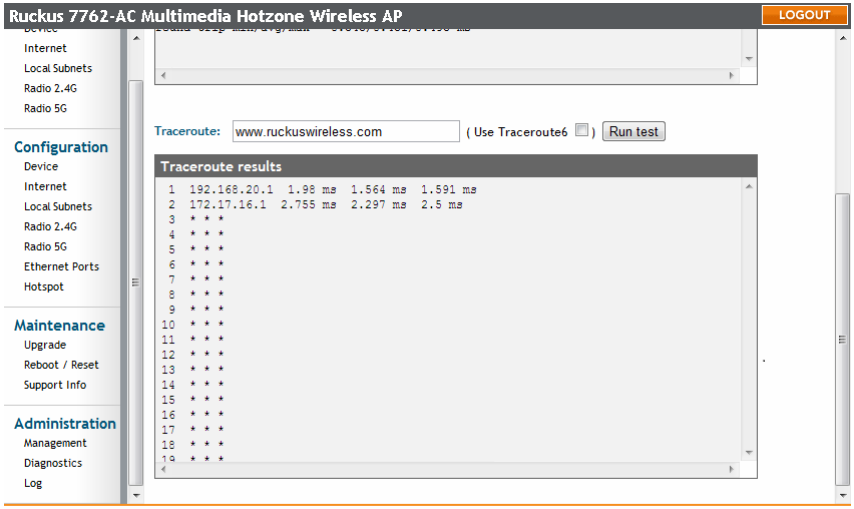


Figure 49. Running traceroute on ruckuswireless.com



Where to Find More Information

If you have questions that this guide does not address, visit the Ruckus Wireless Support Portal at http://support.ruckuswireless.com/. The Support Portal hosts the latest versions of user documentation. You can also find answers to frequently asked questions (FAQs) for each Ruckus Wireless product type.

Index

Numerics

802.1X, 58, 66
802.1X settings, 58
802.1X wired ethernet port, 68

A

access control, 62–63
access point
  event logs, 90
  logs, 90
  management access, other, 85
  managing, 77
  overview, 1
  pointing to FlexMaster, 89
  rebooting, 96
  resetting to factory default, 97
  sending events to a syslog server, 90
  supportinfo.txt, 91
  tr069info.txt, 91
  upgrading firmware
    scheduling automatic, 95
    using a local file, 94
    using FTP or TFTP, 94
    using the web, 94
  ZF 2741, 3
  ZF 7762, 7
  ZF 7762-AC, 16
  ZF 7762-S, 10
  ZF 7762-S-AC, 19
  ZF 7762-T, 13
access point with cable modem
  ZF 7761-CM, 22
access port type, 66
access port, ethernet, 67
access VLAN, 53
administrative computer, 27
administrative login, 84
AeroScout, 48
AP, see access point
associated clients, 83

B

BeamFlex, 1
bridge to L2TP tunnel packet forwarding, 52, 66
bridge to WAN packet forwarding, 52, 66
broadcast SSID, 52

C

cable modem access point
  ZF 7761-CM, 22
changing the login settings, 36
configuring
  access point event logging, 90
  administrative login settings, 84
  device settings, 36
  ethernet port type
    access port, 67
    general port, 67
    trunk port, 67
  ethernet ports
    port-based VLANs, 69
    wired 802.1X, 68
  Hotspot
    basics, 70
    unrestricted access by MAC, 75
    walled garden, 74
  internet settings, 37
    default IP addressing behavior, 39
    L2TP connection, 42
    NTP server and management VLAN, 38
    obtaining and assigning an IP address, 39
  local subnets, 44
  login settings, 36

other management access settings, 85
SNMP management options, 87
syslog settings, 90
TR-069 settings, 87
wireless settings, 46
802.1X, 58
access control, 62
common, 46
rate limiting, 61
threshold options, 60
WEP, 54
wireless #, 51
WPA, 56
connecting an administrative computer, 27
country code, 48, 81
current device settings, viewing, 78
current internet connection settings, viewing, 79
current local subnet settings, viewing, 80
current wireless settings, viewing, 81

D

default IP address, 39
default user name and password, 31
device location, 36
device name, 36
device settings, 36
DHCP
release, 39
renew, 39
DHCP Option 82, 53, 67
diagnostics, 98
disable Ethernet ports, 65
document conventions, i
documentation feedback, ii
dynamic VLAN, 53

E

encryption, 53
ethernet ports
configuration, 65
event logs
access point, 90
saving a copy to your computer, 91
sending a copy to Support using FTP or TFTP, 91

F

factory default, resetting the access point, 97
firmware upgrade, access point
manually using a local file, 94
manually using FTP or TFTP, 94
manually using the web, 94
scheduling automatic, 95
FlexMaster, 1
management status, 88
pointing an access point to, 89
FM, see FlexMaster

G

general port type, 66
general port, ethernet, 67

H

help, 32
Hotspot
basic settings, 70
network settings, 75
optional settings, 71
unrestricted access, 75
walled garden, 74

I

internet settings, 37
IP address, 39
isolated packet forwarding, 52, 66

L

L2TP, 42
local bridging packet forwarding, 66
local subnet, 52, 66
local subnet NAT and route to WAN packet forwarding, 52, 66
local subnets, 44
logging in, 31
logout, 32

M

MAC authentication bypass, 69
management access options, 85
management VLAN, 38
managing access points, 77
menu, 32

N

NTP server, 38

P

packet forwarding, 52, 66
  bridge to L2TP tunnel, 52
  bridge to WAN, 52
  isolated, 52
  local subnet NAT and route to WAN, 52
ping, 98
pointing the access point to FlexMaster, 89
port type, 66
port-based VLAN, 65, 69
protection mode, 50

R

rebooting the access point, 96
related documentation, ii
releasing DHCP, 39
renewing DHCP, 39
resetting the access point to factory default, 97
router mode, 44
Ruckus Wireless
  document feedback, ii
  Support website, 100
  website, 1

S

sending AP events to a syslog server, 90
SSID, 52
Support website, 100
supportinfo.txt, 91
syslog, 90

T

tabs, 32
temperature update, 36
threshold, 52
tr069info.txt, 91
traceroute, 98
transmit power, 50
trunk port type, 66
trunk port, ethernet, 67
tunnel via L2TP, 52
tunnel via L2TP packet forwarding, 66

U

upgrading access point firmware
  scheduling automatic, 95
  using a local file, 94
  using FTP or TFTP, 94
  using the web, 94
user name, 36
using
  ping, 98
  traceroute, 98

V

viewing
  access point wireless mode, 81
  associated clients, 83
  current device settings, 78
  current internet connection settings, 79
  current local subnet settings, 80
  current wireless settings, 81
  FlexMaster TR-069 status, 88
VLAN, 65–66
  overview, 38
  wired, 69
  wireless, 53

W

walled garden, Hotspot, 74
web interface, 31
website
  Ruckus Wireless, 1
  Ruckus Wireless Support, 100
WEP, 54

wireless availability, 52
wireless channel, 47, 81
wireless mode, 47
wireless security
  802.11X, 58
  WEP, 54
  WPA, 56
wireless settings, 46
workspace, 32
WPA, 56
WPA-Auto, 57

Z

ZD, see ZoneDirector
ZF, see ZoneFlex
ZoneDirector, 1
ZoneFlex
  2741, 3
  7761-CM, 22
  7762, 7
  7762-AC, 16
  7762-S, 10
  7762-S-AC, 19
  7762-T, 13
  smart WLAN system, 1